Sicherheitsuntersuchung für einen innovativen Schienenverkehr am Beispiel fahrzeugautarker Ortung

Von der Fakultät für Maschinenbau
der Technischen Universität Carolo-Wilhelmina zu Braunschweig

zur Erlangung der Würde

eines Doktor-Ingenieurs (Dr.-Ing.)

genehmigte Dissertation

von:	Dipl.-Ing. Jörg Christoph May
aus (Geburtsort):	Braunschweig

eingereicht am:	04. Januar 2010
mündliche Prüfung am:	28. Mai 2010
Referenten:	Prof. Dr.-Ing. Dr. h.c. Eckehard Schnieder
	Prof. Dr.-Ing. Jörn Pachl
Vorsitzender:	Prof. Dr.-Ing. Karsten Lemmer

2010

Vorwort

Die vorliegende Dissertation entwickelte sich in den Jahren 2002 bis 2008 aus meiner beruflichen Tätigkeit als wissenschaftlicher Mitarbeiter am Institut für Verkehrssicherheit und Automatisierungstechnik (iVA) der Technischen Universität Braunschweig. Für die thematische Anregung, insbesondere aber für die permanente Förderung dieser Arbeit durch konstruktiv-kritische Betreuung, gilt mein sehr herzlicher Dank in erster Linie dem Institutsleiter, Herrn Prof. Dr.-Ing. Dr. h.c. mult. Eckehard S c h n i e d e r.

Dem Leiter des Instituts für Eisenbahnwesen und Verkehrssicherung der Technischen Universität Braunschweig, Herrn Prof. Dr.-Ing. Jörn P a c h l, danke ich ebenfalls für die anteilige Betreuung und Bereitschaft zur Übernahme des Korreferats.

Meinen ehemaligen Kolleginnen und Kollegen des Instituts bin ich für ihre kooperative Diskussionsbereitschaft dankbar; das gilt insbesondere für den intensiven Gedankenaustausch mit Herrn Dr.-Ing. Jörn D r e w e s.

Meinen Eltern bin ich dankbar für die Förderung meiner Ausbildung und ihr stets gezeigtes Interesse an meiner wissenschaftlichen Tätigkeit. Ganz besonderen Dank schulde ich indes meiner Frau Katja – nicht nur für die fachliche Begleitung, gleichermaßen auch für ihre verständnisvolle Geduld.

Braunschweig, im Mai 2010

INHALTSVERZEICHNIS

KURZFASSUNG

Verkehrssicherheit wird bei Eisenbahnen als dominierende Größe für Qualität und Zuverlässigkeit betrachtet, wodurch der Schienenverkehr seit den Anfängen nicht nur im Volksmund als „sicherstes Verkehrsmittel“ bezeichnet wird. Dieses Sicherheitsniveau wurde durch eine Vielzahl von Erkenntnissen aus Unregelmäßigkeiten im Betrieb sowie durch Iterationsergebnisse bis heute entwickelt. Das daraus entstandene System ist komplex und aufgrund seines dezentralen Vernetzungsgrades nur durch erheblichen Aufwand mit neuen innovativen Ansätzen migrierbar. Hinzu kommt die mitunter schwer durchschaubare Komponentenaufteilung der Systeme auf die beteiligten Ressourcen Infrastruktur und Fahrbetrieb. Da die Ressource Infrastruktur von einer Vielzahl von Verkehrsunternehmen genutzt wird, stellt sich neben der Frage nach der Kostenverteilung auch die Frage: „Wie sicher ist sicher genug“, um letztendlich im Wettbewerb mit anderen Verkehrsarten Nachhaltigkeit zu erlangen.

Einen vielversprechenden Ansatz für einen innovativen Schienenverkehr stellt die fahrzeugautarke Ortung dar. Durch eine Verlagerung der Systemkomponenten von der Infrastruktur auf die Fahrzeuge kann eine Migration mit dem gewachsenen System umgesetzt werden, um Innovationspotenziale für einen wettbewerbsfähigen Schienenverkehr zu nutzen und herauszuarbeiten. Als Grundlage muss das neue Ortungssystem mindestens die gleiche Sicherheit wie das Altsystem aufweisen, weshalb der Fokus dieser Arbeit auf der Untersuchung der Sicherheit liegt und eine durchgängige und strukturierte Methode für eine normkonforme Sicherheitsuntersuchung vorgestellt wird.

Als Referenz wird die schienenfahrzeugautarke Ortung in Verbindung mit dem Betriebsverfahren des Zugleitbetriebs herangezogen, welches in Deutschland für Nebenbahnen sehr häufig Anwendung findet und aus heutiger Sicht die größten Innovationspotenziale aufweist.

Grundlagen der Verkehrssicherheit, der Innovation und des Eisenbahnbetriebs sowie die Betrachtung der Ortung im Schienenverkehr ergänzen die Arbeit.

ABSTRACT

Traffic Safety is regarded to be the dominating factor towards quality and dependability within the Railway Transportation domain. This influenced not only the popular lore regarding railways to be the “safest transportation” among all others from the very first on. This safety level has developed by various expertises collecting from operational irregularities as well as by numerous iterations up to now. The resulting system can only be migrated with innovative approaches with extensive efforts due to its decentralized network and rather complex structure. Furthermore the more or less non-transparent allocation of system components to the involved resources infrastructure and operations emphasizes that. Considering the fact that the resource infrastructure is used by numerous traffic operators (railway undertakings) leads to the question of cost distribution in addition to the question “How safe is safe enough?” in order to achieve sustainability to other traffic modes at last.

A promising approach for an innovative railway traffic solution is given by the vehicle autonomous localisation concept. With the relocation of system components from infrastructure to vehicles the migration with the established system can be realised and thus innovation potentials for a competitive railway transportation system can be developed and used. As a fundamental basis this new localisation system is required to be at least as safe as the existing systems, which brings the safety analysis of this thesis into focus and leads to the introduction of an integrated and structured methodology for safety analysis being compliant to the standards.

The introduced vehicle autonomous localisation in combination with the train control system/mode “Zugleitbetrieb” is used as reference. This train control mode “Zugleitbetrieb” is very common in low density secondary lines in Germany and offers the highest innovation potentials from the current point of view.

Traffic safety basics, innovations in railway operations as well as the consideration of localisation concepts complete this thesis.

1 EINLEITUNG

Das Eisenbahnverkehrssystem hat seit Beginn der Bahnprivatisierung im Jahr 1994 wieder an Bedeutung im „Modal Split“ bezogenen Gesamtverkehr zugenommen. Steigende Energiekosten bei wachsendem Bedürfnis nach Mobilität und Transport im globalisierten Wirtschaftsumfeld verdeutlichen die Notwendigkeit eines leistungsstarken Massenverkehrssystems. Nur durch eine stetige und innovative Weiterentwicklung des Schienenverkehrssystems lassen sich zukünftige Herausforderungen im Verkehrsmarkt nachhaltig bewältigen [Reinhold 2009].

Ein fortschreitender Technologiewandel insbesondere in der Eisenbahnleit- und -sicherungstechnik in Verbindung mit der Harmonisierung der Europäischen Eisenbahnen schaffen geeignete Voraussetzungen, um sich den Herausforderungen zu stellen. Im Vordergrund der Entwicklung steht der gesamte Transportprozess, welcher nur durch Automatisierung leistungsfähiger werden kann. Sicherheit, Leistungsfähigkeit und Kosten sind entscheidende Faktoren, welche die Entwicklung beeinflussen. Das komplexe Zusammenspiel zwischen technischen Einrichtungen und menschlichen Handlungen zur Realisierung der betrieblichen Abläufe im Transportprozess ist daher vorrangig unter Sicherheitsaspekten zu beurteilen, wobei die Berücksichtigung der nachhaltig entstehenden Gesamtkosten für eine Umsetzung kaum eine untergeordnete Rolle spielt. Eine Vielzahl nationaler und Europäischer Vorgaben, Gesetze und Richtlinien bilden den Rahmen für die Betrachtung der Sicherheit bei der Entwicklung der Automatisierung im Schienenverkehr [Suckale 2006], [Müller 2006].

Die große Komplexität des Eisenbahnsystems in Verbindung mit dem Wunsch nach migrationsfähigen Innovationen in eine zum Teil über 100 Jahre alte Technik bei sehr hohen Sicherheitsanforderungen werden in der wissenschaftlichen Fachwelt umfassend dargelegt, um praktikable Lösungsansätze zu finden [Pachl 2004].

Mit dieser Arbeit soll eine sicherheitsgerichtete Untersuchungsmethode für die Innovationsmöglichkeit des Schienenverkehrssystems durch fahrzeugautarke Ortung dargestellt werden, wobei die verschiedenen zu berücksichtigenden Aspekte der Sicherheit und Verlässlichkeit, der Innovation, der Automatisierung, der Gesetzgebung und Richtlinien sowie der methodischen Grundlagen bei der Sicherheitsuntersuchung gegeneinander abzugrenzen sind. Damit soll eine Basis für eine durchgängige und strukturierte Methode für eine Sicherheitsuntersuchung geschaffen werden. Die Methode in exemplarischer Anwendung mit einem innovativen Ansatz für den zukünftigen Schienenverkehr lässt Potenziale für einen innovativen Schienenverkehr ableiten.

1.1 Motivation

Im Eisenbahnwesen ist ein Wandel im Verkehrsaufkommen zu verzeichnen, der – nicht zuletzt hervorgerufen durch ökologische Zwänge bei der Betrachtung des Gesamtverkehrs – der Bahn Wettbewerbsvorteile zurückbringen wird [Ellwanger 2004]. Aufgrund noch fehlender technologischer Offensiven, die in Ansätzen durch die Systemintegration des Europäischen Leit-

und Sicherungssystems ETCS bereits erkennbar sind, kann eine Vormachtstellung gegenüber anderen Verkehrsarten aktuell nur marginal ausgebaut werden. Insbesondere die Ortung der Schienenfahrzeuge als entscheidende Kontaktstelle zwischen der Informationsübertragung zwischen Fahrzeug und Infrastruktur und den (automatisierten) Steuerungen und Sicherungen – sowohl infrastruktur- als auch fahrzeugseitig – kann die entscheidende Basis für eine technologische Offensive in der Automatisierung zu einem leistungsstarken und innovativen Schienenverkehr der Zukunft bieten (Bild 1.1).

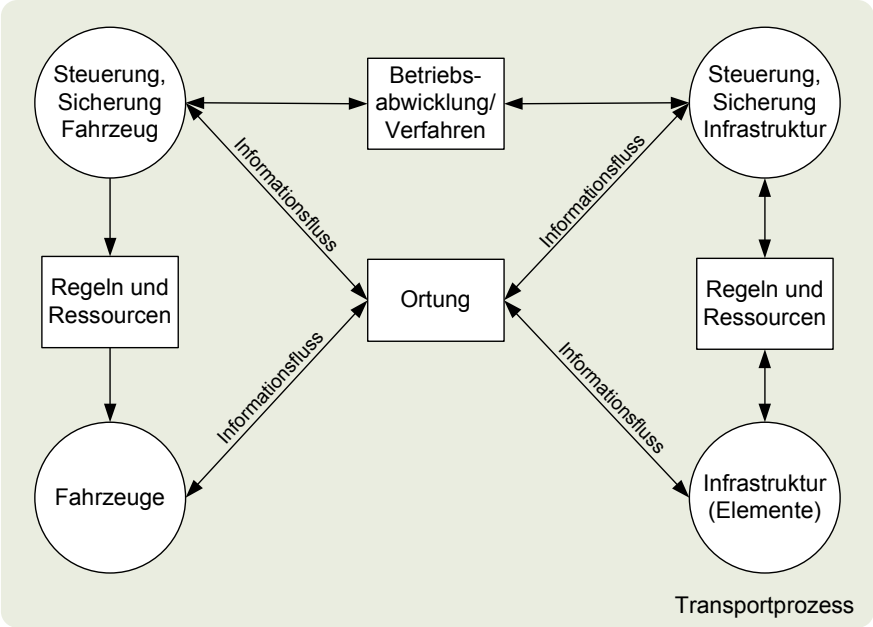

Bild 1.1: Formalisierung der Ortung im Schienenverkehr

Grundsätze der Eisenbahnen waren stets Sicherheit, Pünktlichkeit und Wirtschaftlichkeit in der hier angegebenen Reihenfolge, wodurch die vorrangige Betrachtung der Sicherheit in dieser Arbeit unterstrichen wird.

Wie Quellen belegen, wurden bereits 1838 auf der Strecke der ersten Deutschen Staatseisenbahn zwischen Braunschweig und Wolfenbüttel die ersten „Schnellfahrversuche“ mit einem Zug auf einem Streckenabschnitt durchgeführt, um die Sicherheit des Systems näher zu untersuchen [Schivelbusch 1977]. Geeignete Methoden zur Erstellung von Risikoanalysen, Europäische Richtlinien zur Eisenbahnsicherheit und vieles mehr waren damals selbstverständlich noch nicht bekannt und vorhanden. Allerdings war das System auch noch nicht derart komplex, dass Fahrversuche ohne formale Modellierungshilfsmittel nicht eine genügende Aussage erbracht hätten. Seitdem hat sich das Schienenverkehrssystem erheblich verändert und auch die Untersuchung der sicherheitsrelevanten Funktionen hat sich stetig weiterentwickelt, weshalb insbesondere die Sicherheitsuntersuchung im aktuellen komplexen Systemumfeld eines innovativen Ortungssystems exemplarisch vorangestellt wird.

1.2 Problemstellung

Die Fahrzeugortung im Schienenverkehr ist im gesamten Transportprozess eingebettet in die sicherheitsrelevanten Steuerungs- und Sicherheitsaufgaben und -einrichtungen der Infrastruktur und der Fahrzeuge. Momentan ist die technische Umsetzung der Ortung vornehmlich infrastrukturseitig realisiert, wodurch die Erweiterung der Streckenleistungsfähigkeit stark eingeschränkt ist. Fahrzeugseitige Systeme sind stets in Verbindung mit infrastrukturseitigen Teilsystemen umgesetzt. Auf untergeordneten Nebenbahnen wird die Ortung häufig durch visuelle Prüfungen des Zugschlusses in Verbindung mit mündlichen Rückmeldungen des Betriebspersonals durchgeführt, wobei eine erhöhte Fehleranfälligkeit gegeben ist. Zur bereits genannten Steigerung der Verkehrsaufkommen im Schienenverkehr sind die Vorgaben, nämlich Erhöhung der Leistungsfähigkeit, mindestens gleiche Sicherheit und Reduzierung der Betriebskosten, verträglich in Einklang zu bringen (Bild 1.2).

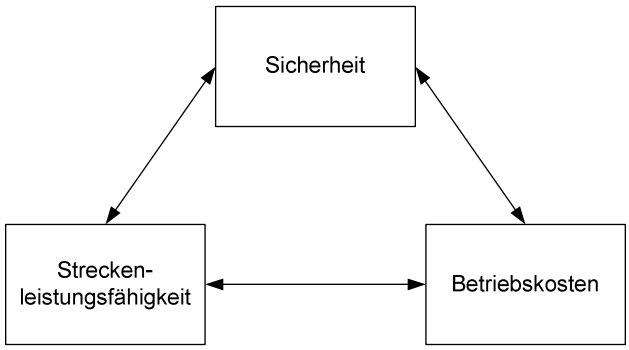

Bild 1.2: Abhängigkeiten für einen innovativen Schienenverkehr

Insbesondere auf Nebenbahnen lassen sich Leistungssteigerungen bei gleicher Sicherheit nicht ohne Investitionen in technische Sicherungseinrichtungen realisieren. In der Vergangenheit haben derartige Überlegungen häufig dazu geführt, untergeordnete Eisenbahnstrecken aufgrund der zu erwartenden höheren Betriebskosten stillzulegen. Mit einer Verlagerung der Ortungseinrichtung als Grundlage einer Sicherheitseinrichtung auf die Fahrzeuge als produktive Elemente könnten bei gleichzeitiger Erhöhung der Leistungsfähigkeit Kosten minimiert und somit langfristig auch wenig befahrene Strecken unter Berücksichtigung der mindestens gleichen Sicherheit betrieben werden.

Hauptbahnen können entsprechend betrachtet werden, wobei sie aufgrund der ohnehin bereits vorhandenen technischen Sicherungsausrüstung – jeweils gestützt durch streckenseitige Ortungseinrichtungen – bereits heute hohe Leistungsfähigkeiten aufweisen. Investitionskosten im Vergleich mit den Betriebskosten spielen bei den intensiv befahrenen Eisenbahnstrecken eine eher untergeordnete Rolle, weshalb exemplarisch in dieser Arbeit vorrangig Nebenbahnen als Untersuchungsfeld herangezogen werden sollen. Sowohl Aspekte der normkonformen Verlässlichkeitsbetrachtung als auch die methodische Sicherheitsuntersuchung für eine innovative

fahrzeugautarke Ortung sollen dabei berücksichtigt werden, um die Zukunft des Schienenverkehrs mit zu gestalten.

Eine Vielzahl weiterer Potenziale bietet die fahrzeugautarke Ortung ergänzend. Dadurch könnten weitere Kostenreduktionen auf allen Strecken nachhaltig realisiert werden.

1.3 Abgrenzung und Zielsetzung

Ziel der Arbeit ist es, eine durchgängige und praxisorientierte Methode für eine normkonforme Sicherheitsuntersuchung im Schienenverkehr zu erarbeiten und mit Hilfe der Betrachtung der Verkehrssicherheit am Beispiel der Ortung vorzustellen, die exemplarisch den Nachweis mindestens der gleichen Sicherheit des fahrzeugautarken Ortungssystems gegenüber dem herkömmlichen leisten kann.

Wissenschaftliches Ziel ist es dabei, den methodischen Ansatz für die Praxisanwendung durch eine exemplarische Validation der Methode zu verdeutlichen. Aufgrund der thematisch ähnlichen Umsetzung der Sicherheitsnachweisführung wird in dieser Arbeit nur das grundsätzliche Vorgehen für generische Anwendungen dargestellt.

Einige Gesamtsystemansätze im Bereich der fahrzeugautarken Ortung werden aktuell erforscht und gehören somit zum Stand der Technik. Auch wurden bereits Ansätze für Sicherheitsuntersuchungen aufgezeigt [Stadlmann 2008]. Eine durchgängige und normkonforme Methode nach CENELEC [EN 50126 ff.] zur Sicherheitsuntersuchung für ein fahrzeugautarkes Ortungssystem ist hingegen neu.

Die vorliegende Arbeit baut auf wissenschaftlichen Vorarbeiten – z.T. unter Beteiligung des Autors – in Projektarbeiten auf, die am Institut für Verkehrssicherheit und Automatisierungstechnik an der Technischen Universität Braunschweig entstanden sind. Relevante Vorarbeiten sind dabei das Projekt „DemoORT“ (Entwicklung eines Demonstrators für Ortungsaufgaben mit Sicherheitsverantwortung im Schienengüterverkehr) mit den Grundlagenarbeiten für einen sicherheitsrelevanten Einsatz und die Basis der Sicherheitsuntersuchung [DemoORT 2007], das Projekt „Hazard-List“ mit der Erstellung einer generischen Gefährdungsliste für Stellwerksanwendungen als Grundlage für Risiko- und Sicherheitsanalysen [Drewes/May 2007] sowie das Projekt „RegioCitadis“ mit der Betrachtung von RAMS-Aspekten für das Bremssystem eines Schienenfahrzeugs [Ständer et al. 2007].

Weitere Vorarbeiten aus dem Bereich der Fahrzeugortung im Schienenverkehr als Grundlage dieser Arbeit waren die Ansätze von [Bikker 1998], [Klinge 1997], [Kirizci 1996], [Leinhos 1996] und [Meyer zu Hörste 2004] sowie einige EU-Vorhaben, die sich mit dem Thema befassen (vgl. Abschnitt 3.5).

1.4 Struktur der Arbeit

Nach der Einleitung wird in den beiden Folgekapiteln der technische Anwendungsbezug als Grundlage zu den Themenfeldern Eisenbahnsystem und -betrieb (Kapitel 2) und Ortung im

Schienenverkehr (Kapitel 3) intensiv vorgestellt. Neben der systemischen Abstraktion werden Automatisierung und Innovation des Schienenverkehrs betrachtet. Legislative Grundlagen werden ebenso wie die betriebliche Abgrenzung von Haupt- und Nebenbahnen in Kapitel 2 herausgestellt. Die Funktionen der Ortung, Systemkomponenten sowie Innovationsansätze, Referenzprojekte und Potenziale der fahrzeugautarken Ortung beinhaltet das Kapitel 3.

Die methodischen Grundlagen der Verlässlichkeit im Schienenverkehr werden in Kapitel 4 als Einstieg in das methodische Konzept der Arbeit aufgeführt. Definitionen im Umfeld der Verkehrssicherheit werden abgegrenzt, auch werden hier die theoretischen Grundlagen der Sicherheitsuntersuchung vorgestellt. Ebenfalls in Kapitel 4 erfolgt eine methodische Abgrenzung und Auswahl geeigneter Beschreibungsmittel für die spätere methodische Anwendung. Auf dieser Grundlage baut die praxisorientierte Methode für eine durchgängige Sicherheitsuntersuchung auf, die in Kapitel 5 in generischer Form vorgestellt wird. Verlässlichkeitsaspekte wie Sicherheitsnachweis und Verfügbarkeitsanalyse sind ebenso theoretisch-methodische Bestandteile dieses Kapitels.

Der methodischen Anwendung und der Bewertung der Sicherheit des innovativen Ortungssystems widmet sich Kapitel 6. Hier wird die Methode aus Kapitel 5 validiert und der Nachweis mindestens gleicher Sicherheit für das fahrzeugautarke Ortungssystem aus Kapitel 3 gegenüber einer Referenzbetrachtung eingeordnet.

Die Zusammenfassung und der Ausblick in Kapitel 7 schließen die Arbeit.

Bild 1.3 gibt einen Gesamtüberblick über die Struktur der Arbeit.

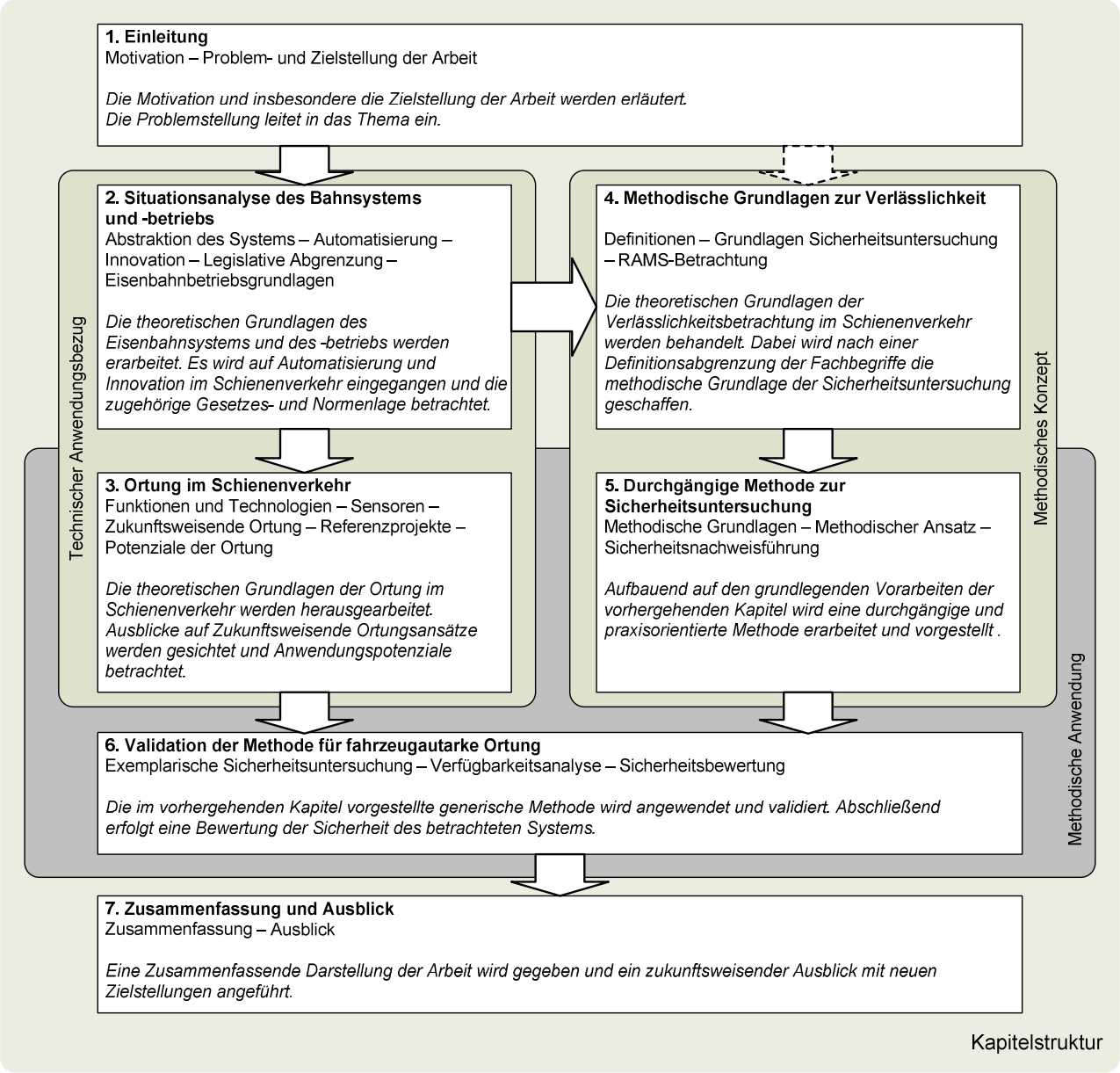

Bild 1.3: Struktur der Arbeit

2 SITUATIONSANALYSE DES BAHNSYSTEMS UND -BETRIEBS

Das System „Eisenbahn“ zeichnet sich insbesondere durch seine zwei hervorzuhebenden Systemeigenschaften, der Spurführung und der langen Bremswege aufgrund geringer Haftreibung zwischen Rad und Schiene aus. Bedingt durch die Spurführung sind bewegliche Fahrwegelemente (Weichen) erforderlich, die durch das System geeignet zu steuern sind. Gleichzeitig müssen die Elemente gegen ungewolltes Umstellen gesichert werden. Die langen Bremswege im Schienenverkehr, die in der Regel die Sichtweiten der Eisenbahnfahrzeugführer um ein Vielfaches übersteigen, erfordern für einen sicheren Betrieb die Regelung und Sicherung der Zugfolge. Daran ist erkennbar, dass das Eisenbahnsystem neben Fahrwegen und Fahrzeugen noch eine Sicherungsebene aufweisen muss, die mit Informationen, wie z.B. Positionsinformationen von Zügen, den sicheren Betrieb gewährleistet. Die Art und Qualität dieser zu übertragenden Informationen ist für die Leistungsfähigkeit des Bahnsystems von Bedeutung, da sie sowohl die Systemsicherheit, als auch die Systemverfügbarkeit beeinflussen kann [Lang et al. 2002], [Schwanhäußer 2009].

Um das System genauer analysieren zu können, wird es im Folgenden abstrahiert, dekomponiert und tiefergehend betrachtet.

2.1 Abstraktion des Systems Eisenbahn

In den frühen Jahren des 19. Jahrhunderts, nachdem die ersten Eisenbahnen ihren Betrieb aufnahmen und die Anzahl der auf einer Strecke verkehrenden Züge anstieg, mussten die Betreiber Lösungen zur Steuerung und Sicherung der Zugfahrten finden. Zunehmend wurden betriebliche Abläufe automatisiert und die Betriebsführungen konzentriert, wodurch menschliche Fehler reduziert wurden und sich die Betriebssicherheit erhöhte.

Das gesamte Eisenbahnsystem besteht aus zwei Teilsystemen, dem grundlegenden der Infrastruktur mit Gleisen, Weichen usw. und dem der darauf verkehrenden Schienenfahrzeuge (vgl. Bild 2.1). Systematisch verknüpft werden beide Teilsysteme durch die Energieversorgung. Teilsystemkomponenten wie Weichen, Gleissperren, Geschwindigkeitsinformationen (z.B. Signale), Ortungseinrichtungen, Bahnübergänge, Zugbeeinflussung etc. sind den Teilsystemen im aktuellen Bahnsystem aufgrund ihrer Realisierungsbeschaffenheit zugeordnet, könnten zum Teil jedoch funktional gesehen auch dem jeweils anderen Teilsystem zugeordnet werden. Die Sicherung der Schienenfahrzeugfahrten auf der Infrastruktur wird durch Stellwerke realisiert, welche erforderliche Informationen der Teilsystemkomponenten bündeln, nach Regeln und Vorgaben logisch verknüpfen und anschließend Steuerungsinformationen den Teilsystemkomponenten in geeigneter Form zur Verfügung stellen.

Mit Einführung der EU-Richtlinie [91/440/EG 1991] sollten sich die Teilsysteme Infrastruktur und Verkehr strikt voneinander trennen, was im Allgemeinen Eisenbahngesetz [AEG 2008] in §9 im Sinne der Trennung von Buchführung und Verwaltung umgesetzt wurde. Aber auch dort wird darauf hingewiesen, dass eine eindeutige Zuordnung unter Umständen nicht immer möglich sein

könnte. Ziele der Einführung der EU-Richtlinie mit der Trennung der Teilsysteme sind die Gewährleistung eines sicheren Betriebs der Eisenbahn und eines attraktiven Verkehrsangebotes auf der Schiene sowie die Sicherstellung eines wirksamen und unverfälschten Wettbewerbs auf der beim Erbringen von Eisenbahnverkehrsleistungen und dem Betrieb von Eisenbahninfrastrukturen. Eine mögliche Bevorzugung einzelner Unternehmen soll damit verhindert werden.

Bei den modernen Eisenbahnen erfolgt aufgrund der Marktöffnung und der Wirtschaftlichkeit eine Trennung zwischen den Eisenbahnverkehrsunternehmen (EVU), welche die Fahrzeuge unterhalten und damit Verkehrsleistungen erbringen, und den Eisenbahninfrastrukturunternehmen (EIU), die die Verkehrswegeinfrastruktur, nämlich das Streckennetz, zur Verfügung stellen und mit Hilfe der den EIU zugehörigen Betriebszentralen den sicheren Betrieb organisieren. Durch diese Trennung der Aufgabenressourcen ergeben sich mit zunehmender technischer Entwicklung Verlagerungs-möglichkeiten von Informationsquellen und -senken, die durch die jeweilige Ressource für wirtschaftliche Vorteile genutzt werden.

Bild 2.1 gibt einen Überblick über das Bahnsystem nach dem formalisierten Prozessmodell [VDI/VDE 3682] in Form eines Petrinetzes, in dem die jeweiligen Teilsysteme als Stellen bzw. Zustände und Ressourcen ausgeführt und entsprechend mit Ereignissen interagierend verknüpft sind. Die hierarchische Gliederung ist in vier betriebliche Ebenen aufgeteilt nach [Erdmann et al. 1994], zuzüglich einer physikalischen Prozessebene. Nach dem Dekompositionsprinzip sind weitere Untergliederungen der einzelnen Funktionen möglich [Fay 1999].

Strategische Ebene:

- EIU und EVU planen mit Hilfe von Verkehrsprognosen und Fahrt- oder Transportaufträgen die Ressourcen an Trassen und Fahrzeugen
- Das EVU bestellt langfristige Trassen beim EIU
- Das EIU entwickelt einen Linienfahrplan
- Die Informationen werden an die Fahrzeug- und Trassenbelegungsplanung übertragen

Im Gesamtsystem wird in dieser Ebene die Formulierung von Zielen, die erreicht werden sollen, durchgeführt. Auf der Basis von Langzeitprognosen werden langfristige Planungen für den Betrieb erstellt.

Dispositive Ebene:

- Das EVU erstellt auf Grundlage der Fahrzeugeinsatzplanung einen Umlaufplan
- Das EIU erstellt auf Grundlage eines Fahrwegplans einen Sollfahrplan
- Die Informationen werden an die Disposition weitergeleitet

Aus betrieblicher Sicht werden in dieser Ebene die Betriebsmittel zur Zielerreichung für die unteren Ebenen bereitgestellt. Betriebswirtschaftliche, technische, logistische Aspekte aber auch Investitions- und Innovationsanregungen werden berücksichtigt und für die Umsetzung vorbereitet.

Taktische Ebene:

- Dispositionsaufgaben werden in der taktischen Ebene behandelt
- Das EVU bestellt kurzfristige Trassen beim EIU
- Das EVU ist für die Fahrzeugdisposition verantwortlich,
  Regeln und Ressourcen sind Vorgaben für das Betriebspersonal
- Das EIU ist für die Streckendisposition in Form der Zugüberwachung verantwortlich
- Als Informationsbasis dient der jeweils aktuelle Istfahrplan

Entsprechend der betrieblichen Disposition werden in dieser Ebene die erforderlichen Betriebsmittel zeitgerecht koordiniert.

Operative Ebene:

- Auf der operativen Ebene wird der sichere Betrieb abgewickelt
- Die Ortung ist die zentrale Funktion in der operativen Ebene und bildet die Informationsquelle für die Steuerungs- und Sicherungssysteme
- Die Ortung überträgt die Positionsinformationen der Fahrzeuge an die Steuerungs- und Sicherungssysteme
- Die Steuerung kann in Stellwerken (Stw.) erfolgen
- Das EVU ist für die Sicherung der Fahrzeuge verantwortlich
- Das EIU ist für die Sicherung der Fahrwege erforderlich
- Kommunikation kann in den Betriebsverfahren automatisiert oder fernmündlich erfolgen

Als Ausführungsebene werden hier die Vorgaben aller übergeordneten Ebenen mit Hilfe der Betriebsmittel umgesetzt. Die Funktion der Fahrzeugortung ist der zentrale Punkt der operativen Ebene.

Physikalische Ebene:

- Die physikalische Ebene wird durch die Fahrzeuge und die Infrastruktur gebildet
- Die Fahrzeuge verkehren auf der Infrastruktur
- Die Ortung ermittelt die relative Position des Fahrzeugs auf der Infrastruktur

Diese Ebene stellt die erforderlichen Betriebsmittel zur Verfügung, in denen Ansätze zur Automatisierung und Innovation gefunden werden können.

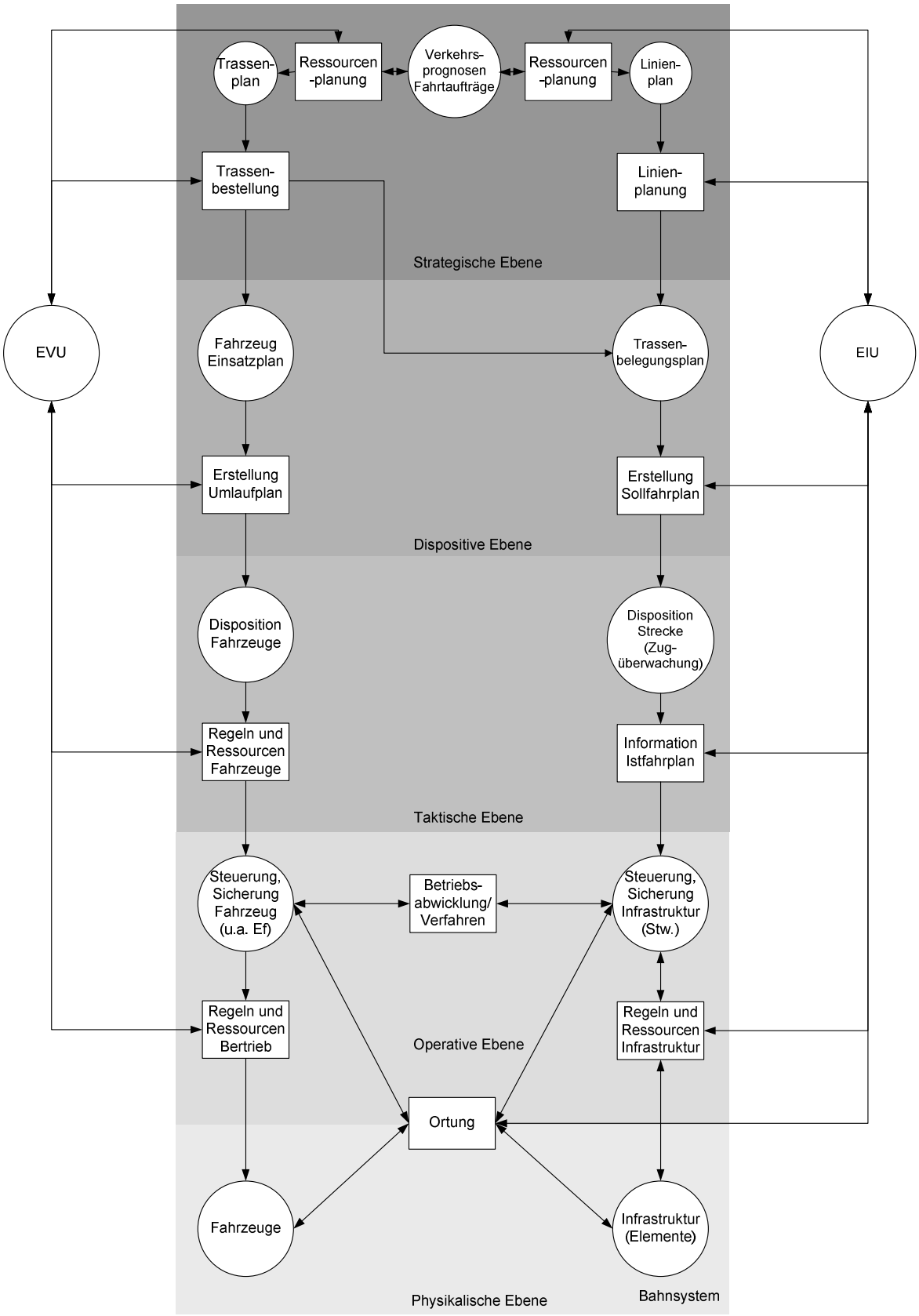

Bild 2.1: Formalisierte Darstellung der Ortung im Kontext des Bahnsystems nach [Fay 1999]

Zur Abgrenzung und Präzisierung der Begriffe wird die „Zugbeeinflussung“ im Folgenden primär als Funktion der fahrwegseitigen Sicherungseinrichtung für eine Zugfahrt definiert. Daten über die

erlaubte Fahrweise werden vom Fahrweg auf das Fahrzeug übertragen und bei Abweichungen entsprechend Schutzreaktionen in Form von Zwangsbremsungen auslöst [Naumann/Pachl 2004].

Die Regelungsfunktion der Zugfahrt kann mit dem Zugbeeinflussungs- und Sicherungssystem unterstützt werden. Der Eisenbahnfahrzeugführer kann in die Funktionsausführung einbezogen werden. Die Terminologie dieses Bereichs ist derzeit noch unscharf [Schnieder 2007].

2.2 Automatisierung im Schienenverkehr

Seit der Inbetriebnahme der ersten Eisenbahnen als Transport- und Verkehrssysteme zu Beginn des 19. Jahrhunderts wurden mit zunehmender Erweiterung der Systeme, begründet durch eine stetige Verkehrszunahme, auch die Teilsysteme komplexer und durch das Personal schwerer beherrschbar. Unfälle waren nicht zu vermeiden und führten zu Lösungsansätzen in Automaten bzw. überwachenden Systemen. Regelungen, Sicherungen und Steuerungen wurden entwickelt und in das Bahnsystem integriert [Pachl 2005]. Die Automatisierung hat sich somit als ein bedeutender Wirtschaftsfaktor im Bereich der Verkehrstechnik entwickelt [Schnieder 1999].

Im Schienenverkehr greift die Automatisierung in den Betriebsablaufs ein und reduziert damit die Verantwortung des Betriebspersonals. Durch eine gesteigerte Automatisierung können Kosten eingespart werden, Investitionen müssen dagegen abgewogen werden. Wenn eine Eisenbahnstrecke nur ein geringes Betriebsleistungsprofil aufweist, führt ein hoher Automatisierungsgrad zu zusätzlichen Kosten. Wenn ein niedriger Automatisierungsgrad mit manuellem Betrieb (gänzlich ohne Automatisierung) mit einem automatischen Streckenblock als größtmögliche Automatisierung gegenübergestellt wird, ergeben sich die exemplarischen Zusammenhänge nach Bild 2.2.

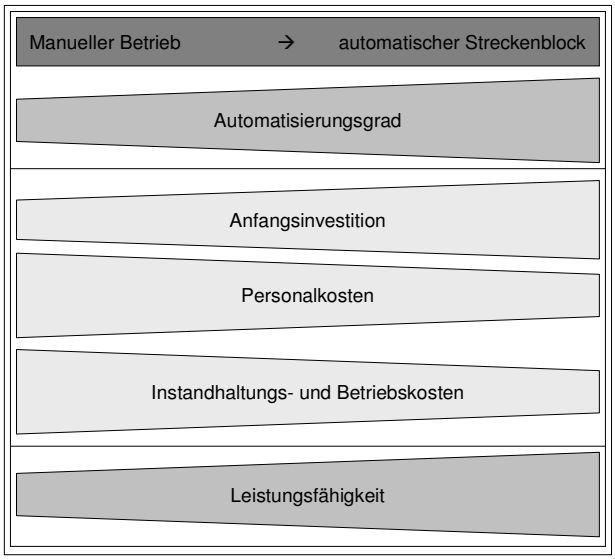

Bild 2.2: Veränderungen durch steigenden Automatisierungsgrad, nach [Meyer zu Hörste 2004]

Als Untersuchungsgegenstände für Automatisierungsansätze im Eisenbahnbereich eignen sich sämtliche Teilsysteme sowohl infrastruktur- als auch fahrzeugseitig, wobei die Teilsystemgrenzen

häufig nicht eindeutig zu definieren sind, was bei der Betrachtung der Ortung und Sicherung deutlich wird (vgl. Kapitel 3).

Zur Erhöhung der gesamten Leistungsfähigkeit im Zusammenhang mit der Steigerung des Automatisierungsgrades entsteht bei Verlagerungen von innovativen Systemteilen von der Infrastruktur auf die Fahrzeuge gleichzeitig auch die Frage nach der Kostenübernahme zwischen den Eisenbahnverkehrsunternehmen (EVU) und Eisenbahninfrastrukturunternehmen (EIU). Somit entstehen, bedingt durch die historische Entwicklung des Systems Eisenbahn, im Zusammenhang mit zukunftsweisenden Ansätzen eines modernen Bahnsystems Konflikte im Bereich von der Kostenzuordnungen und der Nutzen, die insbesondere die Verkehrssicherheit betreffen, da Sicherheit aus primärer Sicht nur Kosten verursacht.

Um den Sachverhalt der Betriebsabwicklung unter den o.a. Umständen zu erläutern zeigt Bild 2.3 die Interaktionen zwischen EIU und EVU.

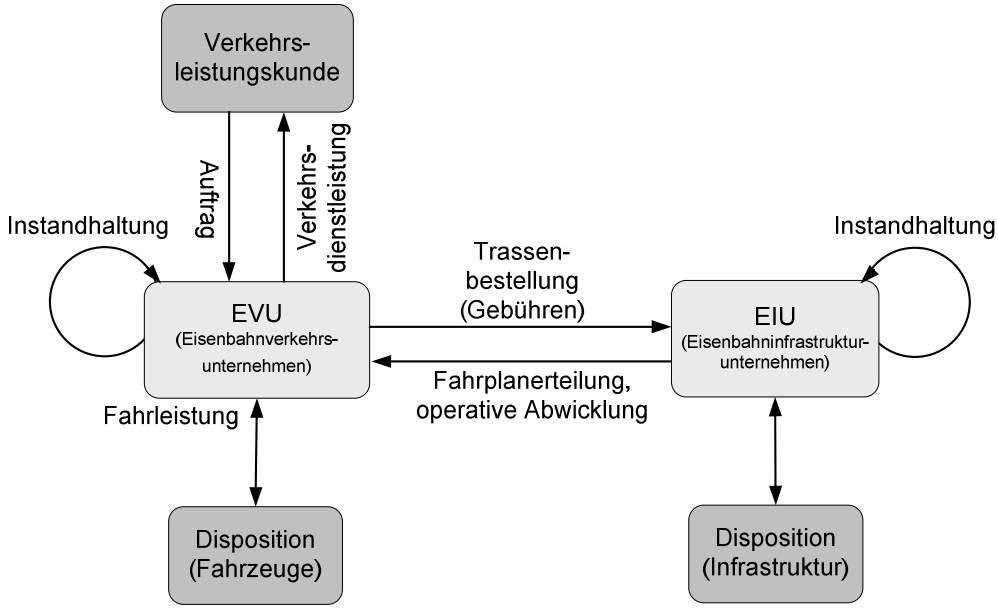

Bild 2.3: Formalisierte Darstellung der Interaktionen im Bahnsystem

Begründet durch die rasche Entwicklung des Eisenbahnsystems in den vergangenen beiden Jahrhunderten wurde eine Vielzahl von Ansätzen zur Automatisierung aufgrund der Erkenntnisse aus Unfällen bzw. Unregelmäßigkeiten im Eisenbahnbetrieb abgeleitet. Die folgenden Stichpunkte geben eine ausgewählte Übersicht über die Vielfältigkeiten der Automatisierungsrealisierungen im Schienenverkehr, unterschieden nach der Fahrzeug-, Fahrweg- oder Betriebsautomatisierung.

Fahrzeug:

- Automatische Fahr- und Bremssteuerung
- Gleit- und Schleuderschutz
- Automatischer Lastwechsel

- Zwangsbremseinrichtungen
- Sicherheitsfahrschaltung
- Zugbeeinflussungssysteme
- Ortungseinrichtung mittels Odometrie
- Ortungseinrichtung mittels Antennen bei Linienzugbeeinflussung
- Automatische Wagenkastenneigung
- Automatische Traktionsabschaltung

Fahrweg:

- Automatisierte Bahnübergänge
- Automatische Achszählung
- Heißläuferortungsanlagen
- Automatische Zugbeeinflussungssysteme
- Rückfallweichen
- Automatische Weichenendlagenerkennung
- Gleisbruchdetektion durch Gleisstromkreise

Betrieb (Steuerung und Regelung):

- Automatische Fahrstraßeneinstellung
- Automatische Fahrwegsicherung
- Automatische Zugfolgeregelung
- Automatisierung von Rangieranlagen und -prozessen
- Automatisierte Zuglaufverfolgung

Sämtliche hier aufgeführten Automatisierungsrealisierungen integrieren sich in das Gesamtsystem und sind jeweils entsprechend der Ausprägung ihrer Kommunikationsschnittstellen zu anderen Systemkomponenten leistungsstark.

Eine relevante Rolle in der Betriebsabwicklung, bezogen auf die Sicherungstechnik, spielt die Positionsinformation des Fahrzeugs in der Bahnautomatisierung. Die Fahrzeugposition, verbunden mit der Information über die Vollständigkeit des Zuges, kann über Sensoren des Fahrwegs, über fahrzeugautarke Technik oder auch in Kombination beider an die Betriebssteuerung übertragen werden. Aufgrund der hervorzuhebenden Relevanz wird in Kapitel 3 die Ortung genauer vorgestellt.

2.3 Innovationen im Schienenverkehr

Aus dem Lateinischen stammend kann der Begriff „Innovation“ grundlegend von novus und innovatio wörtlich zu „Neuerung“ abgeleitet werden. Im deutschen Sprachgebrauch wird der Begriff heute im Sinne von neuen Ideen und Erfindungen sowie für deren wirtschaftliche Umsetzung verwendet. Es bestehen jedoch mehrere Definitionen parallel, da der Begriff sowohl in der Betriebswirtschaftslehre als auch im technischen Bereich Anwendung findet. Allen Definitionsansätzen ist die Verknüpfung des Innovationsbegriffes mit den Merkmalen der Veränderung und der Neuheit eines Produktes oder Prozesses gemein. Aus betriebswirtschaftlicher Sicht ist Innovation die erstmalig wirtschaftlich erfolgreiche Durchsetzung neuer technischer, wirtschaftlicher und sozialer Problemlösungen in einem Unternehmen. Sie ist darauf ausgerichtet, Unternehmensziele auf neuartige Weise zu erfüllen. Aus technischer – und im Bahnsystem auch aus betrieblicher – Sicht sind Innovationen unmittelbar mit Problemlösungsprozessen verbunden. Ein Problem stellt somit eine ungeklärte und widerspruchsvolle Situation dar, die durch qualitativ und quantitativ bestimmbare Differenzen zwischen einem vorhandenen Ist-Zustand und einem notwendigen und wünschenswerten Zielzustand charakterisiert werden kann.

Vorhandene, dem Stand der Technik entsprechende, Standardkenntnisse mit einzelnen Lösungsansätzen reichen zur ganzheitlichen Problemlösung nicht aus, weshalb neue Erkenntnisse und Erfahrungen, neue wissenschaftlich-technische Ergebnisse, technische, wirtschaftliche und soziale Veränderungen zur Überwindung der Differenzen erforderlich sind.

Die Anwendung neuer Wirkprinzipien, wie auch die Neugestaltung von Prozessen und Arbeitsabläufen werden als revolutionäre, sprunghafte Veränderungen bezeichnet. Hingegen ständige, kontinuierliche Verbesserungen bestehender Lösungen oder Prozesse wie auch die Verbesserung einzelner Parameter von Organisationsstrukturen unter Beibehaltung der Prinziplösungen werden als evolutionäre Veränderungen wahrgenommen [Boese 2007].

Eine weitere Differenzierung von Innovationen kann wie folgt festgelegt werden:

- Basisinnovationen beziehen die Anwendung von Schlüsseltechnologien oder neuer Organisationsprinzipien ein. Neue Wirkprinzipien, Produkte oder Verfahren werden entwickelt.
- Verbesserungsinnovationen beziehen sich auf die Verbesserung einzelner oder mehrerer Qualitätsparameter.
- Anpassungsinnovationen beziehen sich auf vorhandene Lösungen, die an spezifische Kundenwünsche angepasst werden.
- Scheininnovationen beziehen sich auf Verbesserungen, welche keinen realen Nutzen erkennen lassen.

Für einen leistungsfähigen und nachhaltig erfolgreichen Schienenverkehr ist somit der Einbezug von Innovationen unbestritten. Mit Blick auf die Ortung können Potenziale abgeleitet werden, die mit innovativen Ansätzen die Nachhaltigkeit und Leistungsfähigkeit des Schienenverkehrs stärken.

Da in Bezug auf die Ortung im Schienenverkehr die Aspekte der Betriebswirtschaft, aber auch der Technik und des Betriebs berücksichtigt werden müssen, gilt es, den bereits dargestellten Ist-Zustand der Ortung einem Zielzustand mit revolutionärer Veränderung durch eine Basisinnovation gegenüberzustellen und die qualitativen und quantitativen Unterschiede herauszuarbeiten.

Seit der anfänglichen Entwicklung der Eisenbahnen gab es eine Vielzahl von Innovationen, die zu einer technischen Reife bis zu Beginn des 20. Jahrhunderts entwickelt waren (vgl. Automatisierungsrealisierungen in Abschnitt 2.2). Dazu zählten insbesondere Fahrzeug-, Fahrweg- und Sicherungssysteme. Seit der Jahrtausendwende sind aufgrund des wachsenden Verkehrsbedarfs und der damit verbundenen Leistungsfähigkeit des Gesamtsystems innovative Ansätze, wie das europäische Zugleit- und Sicherungssystem ETCS (Level 3) mit dem „Fahren im Moving Block“, die Zentralisierung elektronischer Stellwerke in Betriebszentralen, überlange Güterzüge etc. entwickelt und in Ansätzen bereits realisiert worden. Basierend auf der seit 1994 vollzogenen Trennung zwischen der Schienenverkehrswegeinfrastruktur – dem Fahrweg – und den Eisenbahnverkehrsunternehmen, dem eigentlichen Fahrbetrieb, ist es insbesondere aus betriebswirtschaftlichen Gründen erforderlich, innovative Entwicklungen auch nach Fahrweg und Betrieb zu untergliedern. Dieser Ansatz blieb in der Vergangenheit aufgrund der historischen Entwicklung zum gesamtheitlichen Staatsbahnsystem ungeachtet. So wurde die Räumungsprüfung des Fahrwegs bzw. Zugfolgeabschnittes in Verbindung mit der Zugvollständigkeitsprüfung vorrangig technisch fahrwegseitig realisiert. Auch innovative Ansätze, wie die Fahrzeugpositionsermittlung mittels Balisen im Gleis und einer Balisenantenne am Fahrzeug stellen keine Selbstständigkeit dar. Daraus folgend wird die fahrzeugautarke Ortung als eigener Ansatz mit Innovationspotenzial für einen nachhaltigen Schienenverkehr näher untersucht. Aufgrund der primären Zuordnung der Ortung zu sicherheitsrelevanten Anwendungen werden dabei RAMS-Aspekte (RAMS engl. = Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit) [EN 50126] berücksichtigt und soweit möglich den Innovationsansätzen gegenübergestellt.

2.3.1 Ziele der Innovation

Um die zu betrachtenden Inhalte der fahrzeugautarken Ortung näher untersuchen zu können, ist eine Auseinandersetzung mit den Zielen der Innovation erforderlich. Innovationsziele sind dabei insbesondere Qualitätsverbesserungen des Systems, die den Erfordernissen des Kunden entsprechen. Im Fall der fahrzeugautarken Ortung kann der Kunde das fahrzeugbetreibende Eisenbahnverkehrsunternehmen sein, welches durch die innovative Ortung zusätzliche Informationen nutzen kann. Verbesserung von Zuverlässigkeit, Lebensdauer und Sicherheit mit Blick auf das Gesamtsystem sind Größen, synonym den sogenannten RAMS-Kriterien der CENELEC-Normen [EN 50126 ff.].

Ein weiteres Betrachtungsziel ist die Kostensenkung. Eine Innovation ist bei nahezu derselben Funktionalität nur bei gleichzeitiger Kosteneinsparung auf Seiten der Akteure umsetzbar. Eventuelle Erhöhung der Leistungsfähigkeit in Bezug auf das Gesamtsystem, wie auch Erhöhung der Lebensdauer können dabei gegengerechnet werden.

Weitere Ziele aus betriebswirtschaftlicher, rechtlicher und herstellerinterner Sicht sollen an dieser Stelle aufgrund der vorrangig technisch-betrieblichen Betrachtung des Ortungssystems nicht näher vertieft werden. Hier wird daher auf die Literatur verwiesen [Schnieder/Barbu 2009].

Während Produktinnovationen in der Regel darauf abzielen, die Bedürfnisse von Kunden besser zu befriedigen, sind Prozessinnovationen meist auf Verbesserung von Effektivität und Effizienz von Verfahren ausgerichtet. Bei der fahrzeugautarken Ortung kann sowohl von einer Produktinnovation gesprochen werden, sofern das Ortungsmodul als informationsgebendes Produkt aufgefasst wird, als auch von einer Prozessinnovation, da sich die Innovation auf den gesamten Eisenbahnbetriebsprozess auswirkt [Boese 2007].

2.3.2 Innovationsmanagement

Das Management von Innovationen ist Teil der Strategie eines Unternehmens und kann sich auf Produkte, Dienstleistungen, Organisationsstrukturen, Managementprozesse usw. beziehen. In Bezug auf die Ortung für einen innovativen Schienenverkehr sind sämtliche genannten Eigenschaften dabei zu berücksichtigen. Das Innovationsmanagement beinhaltet somit die systematische Planung, Umsetzung und Kontrolle der Idee, in diesem Fall der fahrzeugautarken Ortung. Im Unterschied zur Kreativität, die sich mit der Entwicklung von Ideen beschäftigt, ist das Innovationsmanagement auf die Verwertung der Idee ausgerichtet.

Das Innovationsmanagement umfasst einen Komplex strategischer, taktischer und operativer Aufgaben zur Planung, Organisation und Kontrolle von Innovationsprozessen sowie zur Schaffung der dazu erforderlichen internen bzw. Nutzung der vorhandenen externen Rahmenbedingungen. Grundlegende Aufgaben des Innovationsmanagements sind die Analyse der strategischen Ausgangsposition, die Bestimmung der strategischen Zielposition sowie die Festlegung der Mittel und Wege zur Erreichung der strategischen Ziele [Hauschildt 2007], [Boese 2007].

Zu den allgemeinen Managementfunktionen gehören die Entscheidungen, die zu einer Innovation führen, und sie sind durch folgende spezifische Merkmale gekennzeichnet:

- Komplexität der Entscheidung
- Mehrstufigkeit der Entscheidung
- Zukunftsorientierung der Entscheidung
- Unsicherheit und Risikocharakter
- Kreativität der Entscheidungsträger

In Bild 2.4 sind die fünf Merkmale und deren Abhängigkeiten dargestellt. Jede Größe steht im Zusammenhang mit der Komplexität der Innovationsentscheidung und ist auch bei der fahrzeugautarken Ortung erkennbar.

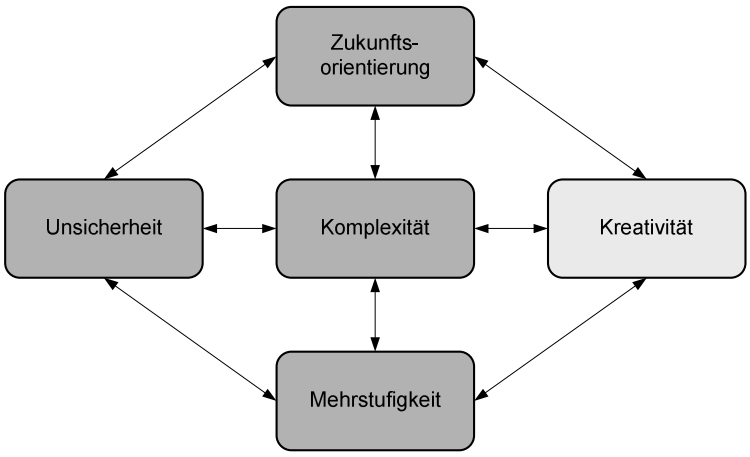

Bild 2.4: Gegenüberstellung der Entscheidungsmerkmale zur Innovation

2.4 Legislative Abgrenzung

Bei signaltechnischen Einrichtungen, wie auch informationsgebenden und -nehmenden Systemen im Zusammenhang mit der Fahrzeug- bzw. Zugposition im Schienenverkehr, stand in der Vergangenheit bei der Beurteilung einer Funktionen vorrangig die Frage nach einer sicheren oder nicht sicheren Systemausführung. Mittels Analysen wurde bestimmt, ob es bei einem technischen Versagen ggf. zu einem Unfall kommen konnte, was es stets zu verhindern galt. Wahrscheinlichkeiten des Auftretens eines gefährlichen Ereignisses sowie Unfallfolgen wurden nicht tiefgründig berücksichtigt. Somit konnte nicht festgestellt werden, wie sicher ein System war und ist, sondern nur, dass es vermeintlich sicher sein könnte. Nach der Einführung einfacher Regeln über anzunehmende und zu beherrschende Fehler, die jeweils durch einen Nachweis der Sicherheit bestätigt werden mussten, wurden mit weiterer Entwicklung bei den Eisenbahnen, u.a. durch Einführung von rechnergestützten Technologien, komplexere Regelwerke erstellt, wie z.B. die „Technischen Grundsätze für die Zulassung von Sicherungsanlagen“ [Mü 8004]. Darin wurden erstmals Ansätze zu differenzierteren Betrachtungsweisen bezüglich der erforderlichen Sicherheit berücksichtigt [Braband 2005].

2.4.1 Normative Grundlagen

Auf Basis der internationalen Norm [IEC 61508] zur Schaffung elektrischer, elektronischer und programmierbarer elektronischer (E/E/PE) Systeme im sicherheitsrelevanten Bereich wurden gegen Ende der 1990er Jahre für den Eisenbahnbereich sogenannte CENELEC-Standards des Europäischen Komitees für elektrotechnische Standards (Comité Européen de Normalisation Electrotechnique = CENELEC) abgeleitet und unter DIN EN 50126, 50128 und insbesondere DIN EN 50129 eingeführt [EN 50126], [EN 50128], [EN 50129]. Mit diesen Normen hat sich für sicherheitsrelevante Systeme eine grundlegende Änderung ergeben. Begriffe wie Risiko- und Gefährdungsanalyse, Risikograph und tolerierbare Gefährdungsrate wurden mit den Normen eingeführt und führten bei der Fachwelt anfangs zu Unsicherheiten [Duczek/Braband 2002]. Für

neue Systeme mit Informations- bzw. Signalübertragungen stellen die Normen aufgrund der detaillierten und phasenorientierten Vorgehensweise eine geeignete Basis dar und lassen Spielraum für innovative Anwendungen im Bahnbereich, da der Grad der Sicherheit des jeweiligen Systems bestimmt und in Relation zu den Kosten dargestellt werden darf [Stanley/Stutzbach 2006].

In Bezug auf die funktionale Sicherheit eines Systems sind, insbesondere für die Durchführung des Sicherheitsnachweises, normative Vorgaben in DIN EN 50129 enthalten. Bezüge zu der phasenorientierten Projektbearbeitung entsprechend des V-Modells sind in DIN EN 50126 aufgeführt. Die sicherheitsrelevante Betrachtung der Software des Systems wird parallel phasenorientiert in DIN EN 50128 abgehandelt. Auf Basis der mittlerweile gewonnenen Erfahrungen mit den CENELEC-Normen werden diese aktuell (Stand 12/2009) überarbeitet und zukünftig in einer Norm zusammengefasst. Eine Erweiterung auf den Anwendungsbereich der Schienenfahrzeugtechnik soll dabei Berücksichtigung finden.

Aufgrund der phasenorientierten Entwicklungs- sowie der parallelen Betrachtungsvorgaben für die Sicherheit sind Einsparungspotenziale bei der Umsetzung innovativer Ideen möglich. Dies gilt nicht nur für Einzelsysteme, wie z.B. ein innovatives Ortungssystem, sondern insbesondere auch für übergeordnete Sicherungssysteme, welche sich positiv auf Streckenleistungsfähigkeiten, Sicherheitsgewinne und Wettbewerbssteigerungen in Verbindung mit geringeren Gesamtkosten auswirken, wodurch der Schienenverkehr nachhaltig wettbewerbsfähig gestaltet werden kann.

Der Vollständigkeit halber sind folgende Standards, Richtlinien und Gesetze bei sicherheitsrelevanten Betrachtungen im Bahnbereich ebenfalls zu berücksichtigen. In den beiden Teilen der DIN EN 50159 [EN 50159] werden zusätzliche Anforderungen für geschlossene und offene sicherheitsrelevante Datenkommunikationen der Systeme definiert. Die Sicherheitsrichtlinie 2004/49/EG [2004/49/EG 2004], verabschiedet von der Europäischen Kommission repräsentiert einen relevanten Schritt zur Harmonisierung der Sicherheit des europäischen Bahnverkehrs. Schwerpunkt ist dabei die Einführung eines einheitlichen Sicherheitsmanagementsystems für Eisenbahnverkehrsunternehmen mit der Erlangung einer Sicherheitsbescheinigung, um die länderspezifischen Regelungen, wie z.B. die Bestellung eines Eisenbahnbetriebsleiters in Deutschland, zu vereinheitlichen und durch einen Sicherheitsmanager zu ersetzen. Gemeinsame Sicherheitsziele (Common Safety Targets), -indikatoren (Common Safety Indicators) sowie -methoden (Common Safety Methods) für alle europäischen Eisenbahnen werden dafür ergänzend eingeführt [2009/352/EG 2009], [Müller 2006].

Als nationales Regelwerk stellt das Allgemeine Eisenbahngesetz (AEG) [AEG 2008] nach dem Grundgesetz die Basis für einen sicheren Eisenbahnbetrieb in Deutschland dar; in §4 werden die Sicherheitspflichten der jeweiligen Parteien behandelt. Mit der Eisenbahn-Bau- und Betriebsordnung [EBO 2008] besteht eine Rechtsverordnung, welche Regelungen enthält, deren Anforderungen durch die Eisenbahnunternehmen erfüllt werden müssen, um einen sicheren Betrieb zu gewährleisten. Die anerkannten Regeln der Technik werden bei der Eisenbahn stets herangezogen, sofern keine Vorschriften verfügbar sind. Zu diesen Regeln oder Gesetzen werden auch geltende

technische Sicherheitsvorschriften und die o.g. CENELEC-Standards zugeordnet [Wittenberg 2002].

Folgende Normen und Gesetze sind als Grundlage für hierarchische Sicherheitsuntersuchungen im Schienenverkehr zu berücksichtigen, welche in schematischer Darstellung auch in Bild 2.5 gezeigt werden.

- IEC EN 61508 (1-3): Funktionale Sicherheit sicherheitsbezogener Systeme

  Diese Norm findet bei sämtlichen Bereichen mit Blick auf sicherheitsbezogene Systeme Anwendung und stellte die Grundlage für die CENELEC-Normen dar. Eine Berücksichtigung des IEC-Standards für eine Systemzertifizierung ist erforderlich, wenn das System nicht speziell im Eisenbahnbereich eingesetzt werden soll.

- DIN EN 50126: Anwendungen im Gesamtsystem Bahn (RAMS)

  Für die Untersuchungen, Spezifikationen und den Nachweis der Verfügbarkeit und insbesondere der Sicherheit (aber auch der Zuverlässigkeit und Instandhaltbarkeit (RAMS)) des Systems ist diese CENELEC-Norm anzuwenden, da das System im Eisenbahnbereich zugelassen werden soll.

- DIN EN 50128: Software für Eisenbahnüberwachungssysteme

  Je nach Betrachtungstiefe der RAMS-Untersuchung ist diese CENELEC-Norm für die Betrachtung der Software im System anzuwenden. Vorgaben und Vorschläge für das methodische Vorgehen beim Nachweis der Sicherheit werden durch eine Übersicht von anzuwendenden Beschreibungsmitteln (und auch Methoden) aufgezeigt, die für die Bearbeitung insgesamt berücksichtigt werden müssen.

- DIN EN 50129: Sicherheitsnachweis für Teil- und Signalsysteme

  In dieser CENELEC-Norm werden Vorgaben zur Durchführung einer Sicherheitsanalyse gestellt. Die Bedingungen für die Sicherheitsanerkennung bzw. -zulassung werden vorgegeben. Eine Berücksichtigung der Norm ist für eine Zulassung somit zwingend erforderlich.

- DIN EN 50155: Elektronische Einrichtungen auf Schienenfahrzeugen

  In dieser Norm werden Vorgaben bezüglich elektronischer Einrichtungen auf Schienenfahrzeugen für ein fahrzeugbasiertes System aufgeführt.

- DIN EN 50159: Sicherheitsrelevante Kommunikation in Übertragungssystemen

  In dieser Norm wird vorgegeben, wie die Kommunikationsübertragungen zwischen den einzelnen Teilsystemen sicherheitskritisch für eine Zulassung betrachtet werden muss.

- VDI/VDE 3681: Einordnung und Bewertung von Beschreibungsmitteln aus der Automatisierungstechnik

In dieser Richtlinie werden ergänzend zur DIN EN 50128 Anregungen zum Einsatz geeigneter Beschreibungsmittel und Methoden u. a. für die Nachweisführung gegeben. Für eine Zulassung ist die Richtlinie nicht relevant, deren Berücksichtigung aber sinnvoll.

- VDI/VDE 3682: Formalisierte Prozessbeschreibung:

  Für die Definition der im System ablaufenden Prozesse in formaler Hinsicht ist die Berücksichtigung dieser Richtlinie ebenfalls sinnvoll, obwohl für eine Zulassung nicht relevant.

- AEG: Allgemeines Eisenbahngesetz

  Als grundlegende Gesetzgebung für die Eisenbahnen in Deutschland steht das AEG. Zulassungsfragen wie auch Zuständigkeiten von Betreibern des Systems sind im AEG geregelt.

- EBO: Eisenbahn-Bau- und Betriebsordnung

  Die EBO regelt nach deutschem Recht den Eisenbahnbetrieb und gibt Aussagen über die Bedingungen für eine Systemzulassung. Die für das System relevante Aussage der EBO ist in §2 (Allgemeine Anforderungen) Absatz (2) enthalten. „Von den anerkannten Regeln der Technik darf abgewichen werden, wenn mindestens die gleiche Sicherheit wie bei Beachtung dieser Regeln nachgewiesen ist.“ (Nachweis gleicher Sicherheit).

  Diese Vorgehensweise entspricht in etwa dem GAMAB-Prinzip (Globalement Au Moins Aussi Bon) nach DIN EN 50126. Das von einem neuen System ausgehende Risiko darf nicht größer als das Risiko eines vergleichbaren, bereits existenten Systems sein.

- BGB: Bürgerliches Gesetzbuch

  Die so genannte Verkehrssicherungspflicht gemäß §823 Absatz 1 BGB ist ebenso zu beachten. Demnach hat derjenige, der in seinem Verantwortungsbereich eine Gefährdungsquelle schafft, Maßnahmen zu ergreifen, die den Schutz der Rechtsgüter Dritter gewährleisten können. Hierbei ist zu prüfen, in wessen Verantwortungsbereich das innovative Ortungssystem fällt. Bei der Einführung neuer Systeme ist nach diesem Gesetz ergänzend zu prüfen, ob sich möglicherweise der Verantwortungsbereich zwischen EVU und EIU verschiebt (Betreiberverantwortung).

Ergänzend sind nicht aufgeführte Vorgaben wie europäische Richtlinien und Verordnungen, Richtlinien der DB AG oder weitere Standardnormen im Literaturverzeichnis aufgenommen.

2.4.2 Zulassungsverfahren

Wegen der Sicherheitsrelevanz eines technischen Systems ist die behördliche Zulassung im Umfeld des Gesamtsystems „Eisenbahn“ bzw. die hoheitliche Inbetriebnahme durch eine Sicherheitsbehörde erforderlich. Die in Deutschland zuständige Aufsichtsbehörde für die Sicherheit im Eisenbahnbereich ist seit 1994 das Eisenbahn-Bundesamt (EBA) mit Sitz in Bonn. Das EBA ist eine

selbstständige deutsche Bundesoberbehörde im Bereich der Bundesverkehrsverwaltung, welche der Fach- und Rechtsaufsicht des Bundesministeriums für Verkehr, Bau und Stadtentwicklung unterliegt. Das EBA ist die Aufsichts- und Genehmigungsbehörde für die Eisenbahnen des Bundes (EdB) und die Eisenbahnverkehrsunternehmen (EVU) mit Sitz im Ausland, bezogen auf das Gebiet der Bundesrepublik Deutschland. Eine hervorzuhebende Aufgabe des EBA ist die Erteilung und Widerrufung von Betriebsgenehmigungen für Systeme und Teilsysteme, wie am Beispiel der sicherheitsrelevanten Ortung [Suwe 2000].

Die normative Legitimation für die – hier relevante deutsche – Zulassungsbetrachtung ist aus der Normenhierarchie (Bild 2.5) abzuleiten. Dem europäischen Recht ist das deutsche Grundgesetz als innerstaatliches Recht mit der so genannten Ewigkeitsgarantie untergeordnet. Auf Grundlage des Grundgesetzes enthält das Allgemeine Eisenbahngesetz (AEG) Aussagen zu Sicherheitspflichten im Eisenbahnbereich und der Zuständigkeit des EBA (§4). Auf Grundlage der Verordnungsermächtigung im AEG (§26) haben die Eisenbahnverordnungen, wie die Eisenbahn-Bau- und Betriebsordnung (EBO), Bestand. In der EBO werden die Regeln zur Sicherheitsbetrachtung verhärtet (§2) [Suckale 2006], [Wittenberg et al. 2004] und [Wittenberg et al. 2006].

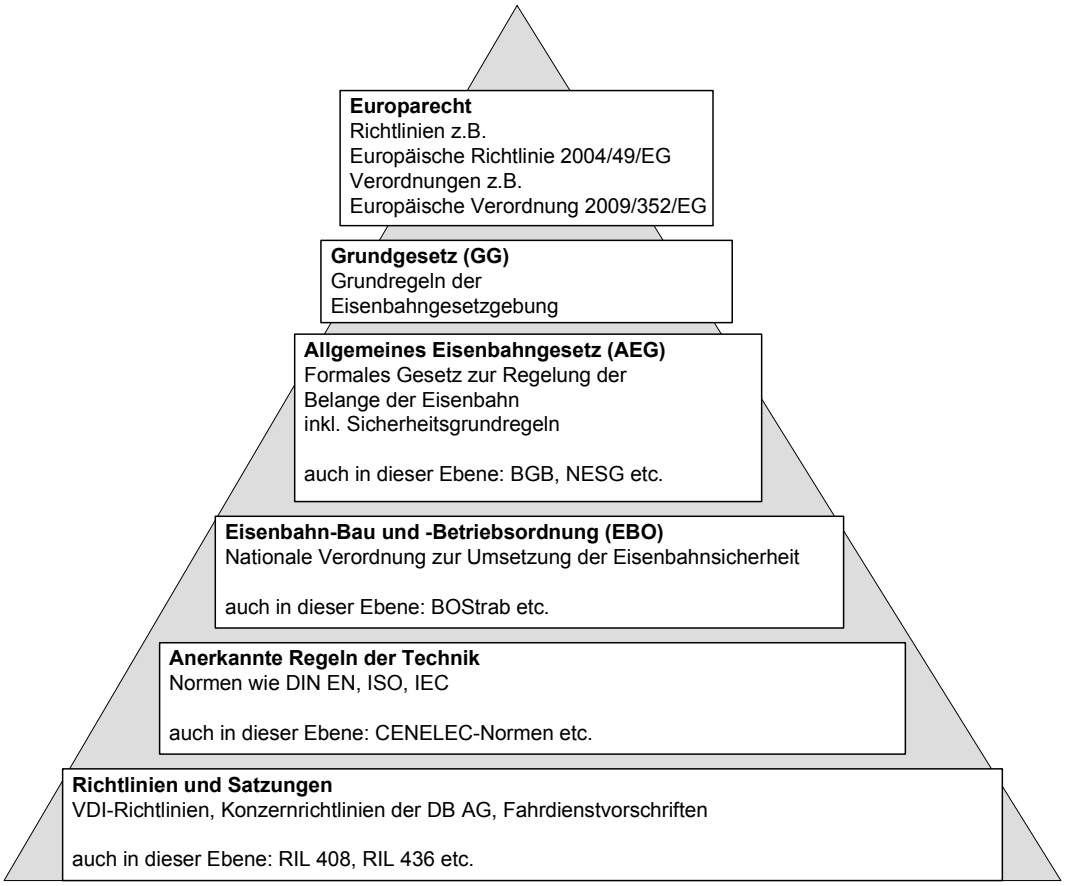

Bild 2.5: Normenhierarchie in Deutschland mit bahnspezifischem Auszug

Sofern die weitere Betrachtung der Zulassung auf Bundesebene verbleibt, können die landesspezifischen Normen unberücksichtigt bleiben. Heranzuziehen sind bei der weiteren

Betrachtung die jeweils gültigen technischen Standards, wie die CENELEC-Normen im Bahnbereich. Abschließend sind noch die betrieblichen Richtlinien der jeweiligen Eisenbahn zu berücksichtigen, bei der z.B. ein fahrzeugautarkes Ortungssystem eingesetzt werden soll. Inhalte der Richtlinien sind u.a. Aussagen über die sicherheitsrelevante Betriebsabwicklung unter Berücksichtigung eines Ortungssystems mit infrastrukturseitiger Zugvollständigkeitsprüfung.

Als Bestandteil der EU-Sicherheitsrichtlinie [2004/49/EG 2004], die in nationales Recht überführt wird, ist die gegenseitige Anerkennung von Systemzulassungen im europäischen Raum verankert. Dadurch wird es zukünftig möglich sein, vereinfacht behördliche Zulassungen in anderen europäischen Ländern zu erhalten, sofern ein sicherheitsrelevantes System bereits in einem europäischen Mitgliedsstaat zugelassen ist.

Nach §6 Abs. 1 der Verordnung über die Interoperabilität des transeuropäischen Eisenbahnsystems [TEIV 2007] bedarf die erstmalige Inbetriebnahme eines strukturellen Teilsystems grundsätzlich einer behördlichen Inbetriebnahmegenehmigung bzw. Zulassung [Galcert 2007].

Für die Beantragung einer Zulassung eines sicherheitsrelevanten Systems sind folgende Unterlagen (Dokumente) bei der zuständigen Aufsichtsbehörde einzureichen:

- Eine ausführliche Beschreibung des Systems einschließlich der geplanten Umsetzungsstrategie sowie des technischen und betrieblichen Rahmens des Systems.
- Die Ergebniszusammenfassung der Sicherheitsanalyse als Grundlage für ein Sicherheitsgutachten.
- Der Sicherheitsnachweis für die Umsetzung des Systems als Grundlage für das Sicherheitsgutachten.
- Der Validierungsbericht als Nachweis der Einhaltung der Sicherheitsanforderungen.
- Ein extern erstelltes Sicherheitsgutachten.

In Bild 2.6 sind zusammenfassend die generischen Anforderungen für den Zulassungsprozess eines sicherheitsrelevanten Systems im Eisenbahnbereich dargestellt.

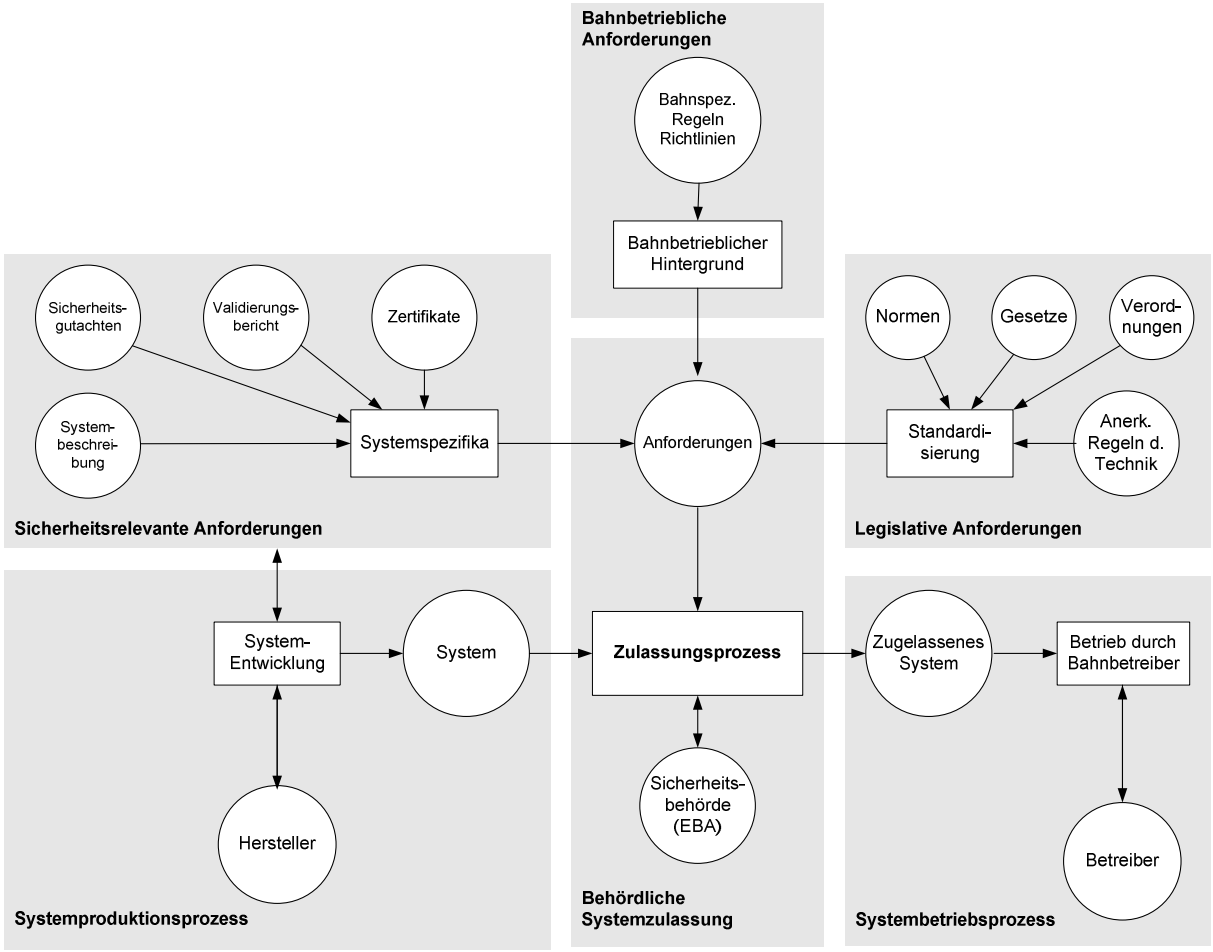

Bild 2.6: Generische Anforderungen für den Zulassungsprozess im Eisenbahnbereich

Grundsätzlich sollte die Sicherheitsbehörde rechtzeitig in den Entwicklungsprozess des Systems mit einbezogen werden, um entsprechend frühzeitig auf Mängel in Dokumenten hinweisen zu können. Iterationsschritte in späteren Phasen können dadurch vermieden werden.

2.4.3 Zertifizierung von Teilsystemen und Akkreditierung

Aufgrund des Neuheits- und Innovationsgrades des Ortungssystems sind im Vorfeld einer Zulassung umfangreiche Systemtests durchzuführen, die den Nachweis der Sicherheit plausibilisieren. Diese umfangreichen Tests können mit der Zertifizierung des Systems oder Teilen davon abgeschlossen werden. Das Ergebnis der Zertifizierung geht dann ebenso in die einzureichenden Unterlagen mit ein und kann den Zulassungsprozess vereinfachen bzw. beschleunigen.

Als Zertifizierung wird ein Prozess bezeichnet, mit dessen Hilfe die Einhaltung vorgegebener Standards für Produkte (bzw. Dienstleistungen) und ihre jeweiligen Herstellungsverfahren nachgewiesen werden kann. Die Zertifizierung besteht im Allgemeinen in der Ausstellung eines Zeugnisses bzw. Zertifikats. In Abgrenzung zum o.a. behördlichen Zulassungsprozess kann die Zertifizierung auch als Teilsystemzulassung bezeichnet und durch unabhängige, akkreditierte

Institutionen durchgeführt werden; der Begriff „Zulassung“ bezieht sich dann auf die Integration in ein Systemgesamtumfeld.

In Abgrenzung dazu steht der Begriff der Akkreditierung (lat. accredere, Glauben schenken), welcher die Situation umschreibt, dass eine allgemein anerkannte Instanz oder Aufsichtsbehörde einer anderen Institution das Erfüllen einer besonderen (nützlichen) Eigenschaft bescheinigt. Die Akkreditierung stellt dabei nicht die Bescheinigung des Endergebnisses dar [Hänsel 2008].

Für die Zertifizierung des innovativen Ortungssystems für einen sicherheitsrelevanten Einsatz im Gesamtsystem Bahn sind – aufgrund der Systemneuheit ohne geeignete Referenzen – ergänzend zum o.a. Prozess umfangreiche Versuche und Tests im Vorfeld durchzuführen und Dokumentationen zu prüfen, um die Einhaltung der vorgegebenen Normen nachzuweisen. Zertifizierungen der Konformität zum Qualitätsmanagementsystem sowie zur CENELEC-Entwicklung wären denkbare Ansätze. Als Bestätigung können durch akkreditierte Institutionen Zertifikate ausgestellt werden, welche als Bestandteil der Zulassungsunterlagen Berücksichtigung finden [Galcert 2007].

Im Rahmen der exemplarischen Teilsystemzertifizierung gelten mindestens ergänzend nachstehende Erfordernisse:

- Für ein sicherheitsrelevantes, fahrzeugautarkes Ortungssystem, welches in Verbindung mit einem Sicherungssystem zugelassen werden soll, muss nachgewiesen werden, dass das Teilsystem plan- und genehmigungskonform entwickelt wurde. Diese Informationen sind in einem Sicherheitsbericht zusammenzustellen.
- Ein Nachweis über die Einhaltung relevanter Vorschriften und weiterer Rechtsvorschriften, deren Anwendung für die Erfüllung der grundlegenden System- und Sicherheitsanforderungen erforderlich sind, ist zu erbringen.

Bild 2.7 gibt einen Überblick über den Zertifizierungsprozess eines generischen Teilsystems. Zum Abgleich des Systems sollte in einem Testlabor ein Referenzsystem verfügbar sein, welches für die Untersuchungen zur Zertifizierung herangezogen wird. Das Testlabor bzw. der unabhängige Sachverständige selbst muss wiederum durch die Aufsichtsbehörde akkreditiert sein. Nach erfolgten Tests und positivem Abgleich mit standardisierten Vorgaben erfolgt letztlich die durch das akkreditierte Labor vorbereitete technische Zertifizierung durch die Aufsichtsbehörde, die – in Verbindung mit der Integration in das Gesamtsystemumfeld – der behördlichen Zulassung entspricht.

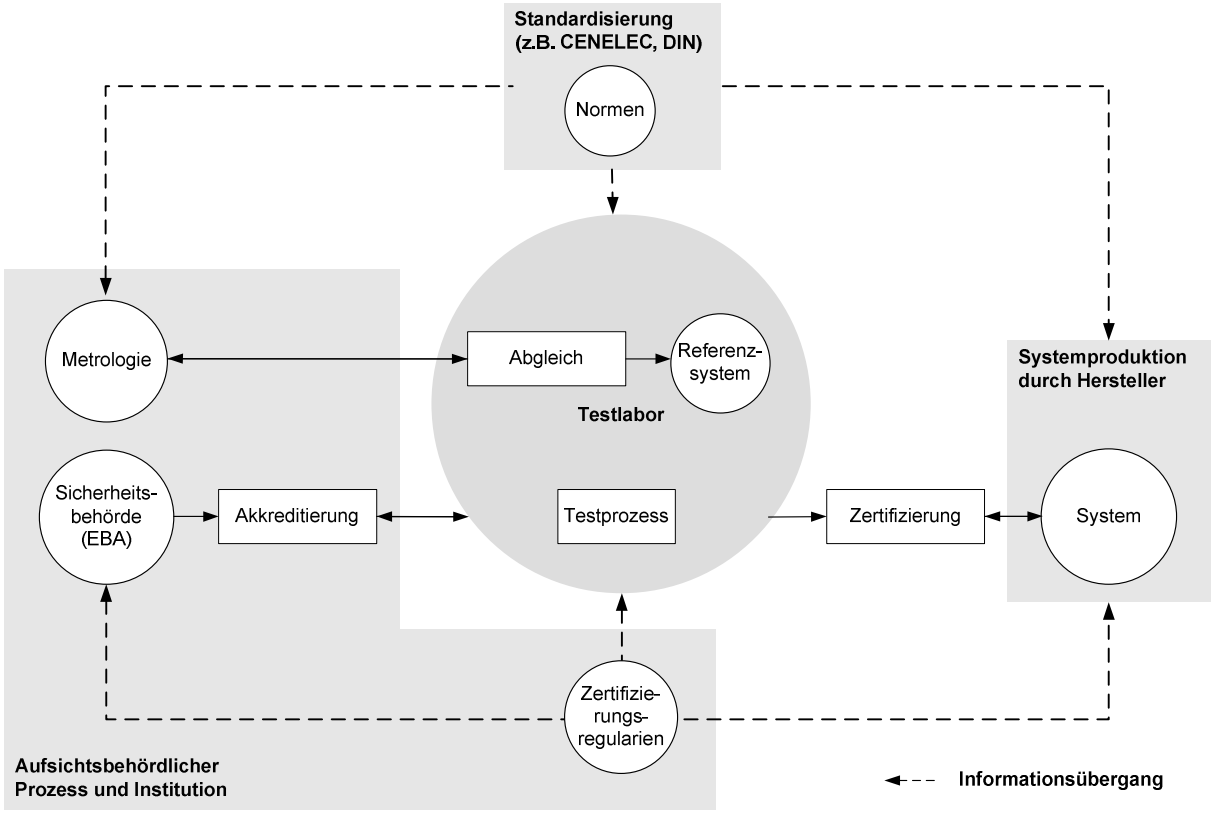

Bild 2.7: Generische Prozessdarstellung der Zertifizierung

Nach erfolgter Zertifizierung und behördlicher Zulassung des Gesamtsystems steht dem Einsatz im Eisenbahnbetrieb nichts mehr entgegen. Durch die Zertifizierung in den vorgenannten Bereichen können die Qualität, Sicherheit und Zuverlässigkeit des betrachteten Systems bestätigt werden. Die Innovationsparameter der Kosteneinsparung und Qualitätsverbesserung mit der Erhöhung der Leistungsfähigkeit und Lebensdauer lassen sich daraus ableiten.

Um die potenziellen Kosteneinsparungen zu betrachten, müsste der Neubau von Eisenbahnstrecken mit herkömmlichen Ortungs- und Sicherungssystemen dem Umbau von Strecken und der Ausrüstung von Fahrzeugen mit dem innovativen Ortungs- und Sicherungssystem im Kosten-Nutzen-Vergleich der Leistungsfähigkeiten gegenübergestellt werden. Eine schnellere Amortisierung des innovativen Systemansatzes bei gleichzeitig geringerem Verbrauch von Landschaftressourcen lässt sich bereits heute überschlägig ableiten. Die Diskussion über die Kostenverteilung zwischen den zukünftigen fahrzeug- und streckenseitigen Systemaufteilungen muss mit Hilfe von Kosten-/Nutzenanalysen geführt werden, um eine sinnvolle Aufteilung auf alle Systemteilhaber des zukünftigen erfolgreichen Schienenverkehrs zu erreichen [Thiele 2008].

2.5 Eisenbahnbetriebsgrundlagen

Seit jeher ist es in erster Linie Aufgabe der Stellwerke bzw. deren technisch umgesetzter Logik, die Sicherung des Betriebes der Fahrzeuge auf der Infrastruktur zu gewährleisten. Mit Hilfe der Logik werden Fahrweg- und Zugfolgesicherungen umgesetzt, insbesondere wird sicher gestellt, dass der

zu einer Fahrstraße gehörende Fahrweg verschlossen und die jeweils richtige Geschwindigkeitsinformation als Signalbegriff übertragen wird. Ein Fahrweg stellt eine Fahrmöglichkeit für ein Schienenfahrzeug dar, die sich aus der Lage der Weichen und der zugehörigen Gleise in der Topologie eines Gleisnetzes ergibt; von einer Fahrstraße (Zug- oder Rangierstraße) wird gesprochen, wenn ein bestimmter Fahrweg durch das Stellwerk sicherungstechnisch für eine Zug- oder Rangierfahrt freigegeben ist. Für jede Zugfahrt wird entsprechend eine neue Fahrstraße eingestellt, so dass die Zugfahrt als Folge technisch gesichert ablaufen kann. Um den Betrieb mit Hilfe der vorgenannten Kenngrößen sicher durchführen zu können, sind auch Informationen über die Position des Zuges und seine Vollständigkeit erforderlich, die ebenfalls u.a. im Stellwerk umgesetzt werden.

Die Betrachtung des (deutschen) Eisenbahnbetriebes bedingt die Betrachtung der legislativen Grundlagen und Vorgaben aus Betriebsordnungen. Unterschiede und somit Ansätze für Innovations- und Automatisierungsbetrachtungen bestehen in verschiedenen Kategorien von Eisenbahnstrecken in Abhängigkeit von der vorhandenen Sicherungstechnik sowie in – darauf aufbauend – unterschiedlichen Betriebsverfahren bzw. umgekehrt. Eine Folgebedingung sind die daraus resultierenden ungleichen Sicherheitsebenen.

2.5.1 Streckenklassifikation

Die für in Deutschland tätigen Eisenbahnverkehrs- und Infrastrukturunternehmen zu beachtende Eisenbahn-Bau- und Betriebsordnung (EBO) [EBO 2008] unterteilt in §1 (2) Eisenbahnstrecken in Haupt- und Nebenbahnen. Umgangssprachlich werden häufig auch die Begriffe „Nebenstrecke“ und „Regionalstrecke“ für Nebenbahnen mit untergeordneter Bedeutung und geringer Verkehrsleistung verwendet [Zimmer 2002]. Die herausstechenden Charakteristika von Nebenbahnen sind Bahnhofs- bzw. Haltepunktabstände von durchschnittlich drei bis fünf km, Streckenhöchstgeschwindigkeiten von 80 km/h, eine vereinfachte bis keine sicherungstechnische Ausrüstung und in der Regel eine eingleisige Betriebsführung. Somit kann auch von einfachen betrieblichen Verhältnissen gesprochen werden. Auf Nebenbahnen ist nach EBO eine Vielzahl von Vereinfachungen in Bezug auf bauliche und signaltechnische Realisierungen gegenüber Hauptbahnen zugelassen. Hauptbahnen sind entsprechend sicherungstechnisch für einen höherwertigen Betrieb ausgerüstet.

Bild 2.8 zeigt einen Überblick über die Unterschiede zwischen Haupt- und Nebenbahnen nach EBO.

Streckenmerkmal	Hauptbahn	Nebenbahn
Zulässige Geschwindigkeit	bis 250 km/h (nach Sicherungstechnik)	bis 80 km/h (bis 100 km/h bei signal. ZLB)
Zugbeeinflussung	wenn v > 100 km/h	nicht vorhanden
Signalausrüstung	vorhanden	ggf. nicht vorhanden
Einfahrsignale	vorhanden	wenn v > 50 km/h
Ausfahrsignale	vorhanden	wenn v > 60 km/h
Einfahrvorsignale	wenn v > 60 km/h	wenn v > 60 km/h
Signalabhängigkeit von Weichen	vorhanden	wenn v > 50 km/h
Ortsinformationsübertragung	technisch über Sensoren	fernmündlich über Personal
Achslast bei Streckenneubau	mindestens 25 t	mindestens 16 t
Gleisbogenradien	minimal 300 m	minimal 180 m
Längsneigung auf freier Strecke bei Neubauten	≤ 12,5 ‰	≤ 40 ‰
Streckenanteil	ca. 70 %	ca. 30 %

Bild 2.8: Charakteristika von Haupt- und Nebenbahnen in Deutschland

Eine ergänzende Unterscheidung der Streckencharakteristika kann in Bezug auf die Spurweite, die Sicherungstechnik an Bahnübergängen, Signale und Weichen sowie integrierte Zugbeeinflussungssysteme vorgenommen werden. Die letztendliche Entscheidung darüber, welche Strecken als Haupt- oder Nebenbahn gelten, trifft der Bundesminister für Verkehr [Naumann/Pachl 2004].

Etwa 40% der europäischen Eisenbahnstrecken weisen den Charakter von Nebenbahnen auf. Diese Verteilung ist in Deutschland mit ca. 30 % Nebenstreckenanteil in etwa konform; die Gesamtlänge des deutschen Eisenbahnnetzes beträgt mit Stand vom März 2006: 34.128 km, wovon etwa 10.000 km als Nebenbahnen ausgewiesen sind [Verkehr 2007]. Die betriebliche Abwicklung des Verkehrs auf den jeweiligen Bahnen ist primär von der technischen Ausrüstung der Sicherungstechnik abhängig. Die in Deutschland angewendeten Betriebsverfahren sind für Hauptbahnen und mit etwa 2.600 km der Nebenbahnen [Lenz 1999] das Standardverfahren [Naumann/Pachl 2004] und ausschließlich für Nebenbahnen der Zugleitbetrieb (ZLB) [RIL 436] oder der signalisierte Zugleitbetrieb (SZB) nach [RIL 437]. Eine tiefergehende Betrachtung der Betriebsverfahren ist in Abschnitt 2.5.2 enthalten.

Aufgrund der aufgezeigten Charakteristika der Nebenbahnen ist die Leistungsfähigkeit auf derartigen Eisenbahnstrecken eingeschränkt, was in der Vergangenheit bereits zu einer Vielzahl von Streckenstilllegungen, begründet mit Unwirtschaftlichkeit, geführt hat. Wie bereits erläutert sind die betrieblichen Verhältnisse der Strecken nicht zuletzt durch einfache Ausrüstungen der Sicherungstechnik begründet, wodurch ein sicherer Betrieb nur aufgrund von Leistungs- bzw. Verfügbarkeitseinschränkungen durchgeführt werden kann. Ein entscheidendes Kriterium für die Leistungs-

fähigkeit ist die Ortung der Züge auf Nebenbahnen, die nahezu flächendeckend durch Personaleinsatz im Zugleitbetrieb durch z.B. Zuglaufmeldungen abgewickelt wird. Daraus resultiert die Notwendigkeit der Betrachtung der sicherheitsrelevanten Ortung für innovative Automatisierungsansätze zur Leistungssteigerung und Erhaltung von Nebenbahnen.

2.5.2 Zugbeeinflussung und Folgefahrschutz in Betriebsverfahren

Bedingt durch die mäßigen Bremseigenschaften der Schienenfahrzeuge aufgrund des geringen Haftreibungsbeiwertes (Stahl auf Stahl für das Rad/Schiene-System), sind ohne technische Sicherungseinrichtungen Unfälle aufgrund menschlichen Versagens, insbesondere hervorgerufen durch Triebfahrzeugpersonal kaum zu verhindern. Gegen Ende des 19. Jahrhunderts wurden verstärkt Untersuchungen zur Verbesserung der Sicherheit durchgeführt, die mit Automatisierungsansätzen für den Schienenverkehr gekoppelt waren. Die durch Signale optisch an das Fahrpersonal übermittelten Informationen über die zulässige Geschwindigkeit wurden schließlich zusätzlich mechanisch, elektrisch oder induktiv auf die Triebfahrzeuge übertragen und zur Überwachung des Triebfahrzeugpersonals genutzt. Bei Nichtbeachtung eines Signals oder falscher Reaktion hatte das technische System die Aufgabe, automatisch eine Zwangsbremsung des Zuges zu bewirken und somit den Zug in einen sicheren Zustand zu überführen. In Deutschland konnte sich eine induktive Lösung eines Zugbeeinflussungssystems unter der Bezeichnung „INDUSI“ (Induktive Zugsicherung) ab Beginn der 1930er Jahre durchsetzen. In nennenswerter Zahl wurde das System jedoch erst ab den 1950er Jahren auf den Eisenbahnstrecken installiert und findet auch heute großflächig vor allem auf Hauptbahnen Anwendung [Schnieder 2007].

Um einen Eisenbahnbetrieb effizient durchführen zu können ist neben den genannten Sicherungsaspekten die Abstandshaltung zwischen zwei fahrenden Zügen genauer zu untersuchen. Die wesentlichen Kenngrößen sind die dynamischen Parameter des Zuges „Geschwindigkeit und Fahrzeugbeschleunigung“ als fahrzeugbedingte Größen sowie die streckenbedingten Größen der Fahrwegtopologie und des Betriebs. Tiefer gehend wird die Theorie der Abstandshaltung und ihrer Auswirkungen auf den Eisenbahnbetrieb in Betriebsverfahren u.a. von [Pachl 2004] und [Schnieder 2007] betrachtet.

In der Realisierung der Abstandhaltung wurden im Schienenverkehr folgende Verfahren als Grundlage für die Zugbeeinflussung und den Folgefahrschutz angewendet und in Betriebsverfahren integriert:

Fahren im Zeitabstand

Der zeitliche Mindestabstand zwischen zwei Zügen ($f(t_{FolgeZUGt})$) ist als Funktion der Folgezugzeit vorgeschrieben. Eine technische Überwachung, ob der vorausfahrende Zug die Strecke vollständig geräumt hat, besteht jedoch nicht. Aufgrund der Risiken und der eingeschränkten Verfügbarkeit der Strecken wird dieses Verfahren seit Ende des 19. Jahrhunderts in Europa nicht mehr angewendet [Pachl 2004].

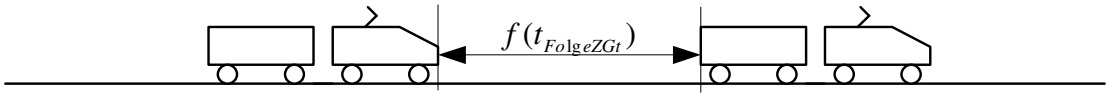

Bild 2.9: Fahren im Zeitabstand

Fahren im absoluten Bremswegabstand

Aus dem Bremsweg des Folgezuges 2 ($l_{B,\ Zug\ 2}$) und einem Sicherheitszuschlag (S) lässt sich der Abstand zwischen den beiden Zügen errechnen. Bei dieser Abstandshaltung stellt der Zugschluss des Zuges 1 einen sich bewegenden Gefahrpunkt dar. Ortsfeste Gefahrpunkte, wie z.B. Weichen, sind ebenso durch Bremsweg und Sicherheitszuschlag zu betrachten. Der Sicherheitszuschlag kann an dieser Stelle mit der Ortungsungenauigkeit gleichgesetzt werden, womit dieses Verfahren als Betrachtungsgrundlage für den Zugleitbetrieb auf Nebenbahnen dienen kann. Mit zunehmender Fahrgeschwindigkeit verlängert sich auch der Bremswegabstand zum Gefahrpunkt, wodurch sich auch die Ortungsungenauigkeit erhöht.

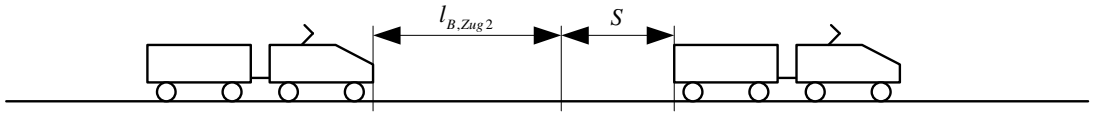

Bild 2.10: Abstandshaltung durch absoluten Bremswegabstand

Fahren im relativen Bremswegabstand

Der Abstand zwischen Zug 1 und Zug 2 ergibt sich aus der Bremswegdifferenz der sich überlagernden geschwindigkeitsabhängigen Bremswege der beiden Züge sA ($sA = l_{B,\ Zug\ 2} - l_{B,\ Zug\ 1} + S$) unter Berücksichtigung der Bremsverzögerungen und einem Sicherheitszuschlag.

Dieses Verfahren ist aus dem Straßen- oder auch Straßenbahnverkehr als gebräuchliches Abstandshalteverfahren bekannt. Im Schienenverkehr wird bei Eisenbahnen dieses Verfahren ggf. nur im Rangierdienst im Sichtfahrbereich angewendet, da auf den Strecken aufgrund der streckenseitigen Ortung in Verbindung mit dem geringen Bremsvermögen der Fahrzeuge keine geeigneten technischen Sicherungssysteme existieren.

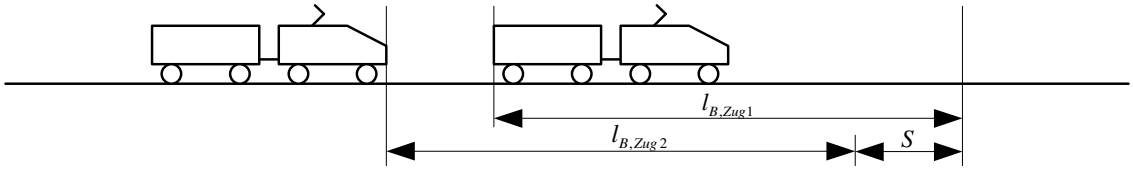

Bild 2.11: Abstandshaltung durch relativen Bremswegabstand

Fahren im festen Raumabstand

Der Abstand zwischen zwei aufeinander folgenden Zügen von mindestens dem maximalen Bremsweg bei höchstzulässiger Streckengeschwindigkeit und einem Sicherheitszuschlag wird als konstanter Raum freigehalten. Aufgrund der im Standardverfahren gebräuchlichen Realisierung einer ortsfesten Signalisierung mit sogenannten Blockabschnitten wird jeweils der Blockabschnitt als Raumabstand zwischen zwei Zügen freigehalten. Als Sicherheitszuschlag wird in einem auf den Block folgenden Bereich ein Durchrutschweg einbezogen [Pachl 2004].

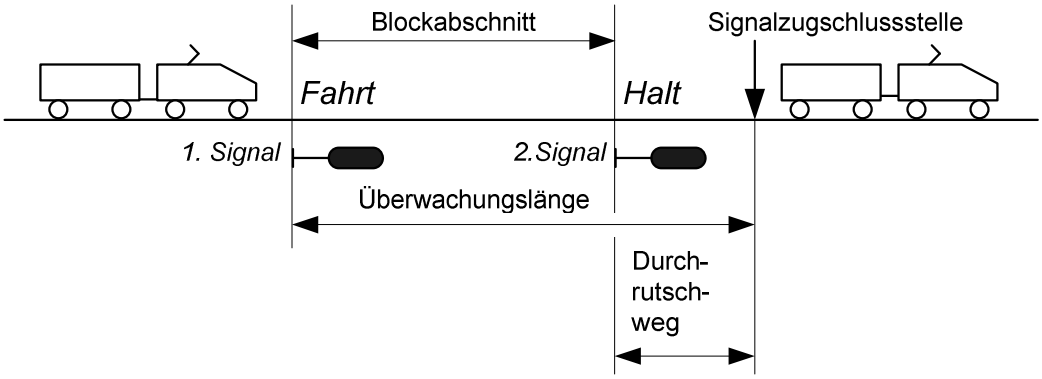

Bild 2.12: Abstandshaltung durch festen Raumabstand

Die Grundprinzipien „Sicherheit, Pünktlichkeit und Wirtschaftlichkeit“ sind für den Eisenbahnbetrieb in der genannten Reihenfolge die primären Größen. Um diese effizient in Einklang zu bringen, sind sogenannte Betriebsverfahren für die Abwicklung des Betriebes auf Haupt- und Nebenbahnen in unterschiedlichen Anpassungen entwickelt worden [Gutsche 2009]. Wie im vorherigen Abschnitt kurz angedeutet, wird für den Betrieb auf Nebenbahnen vorrangig das Verfahren des Zugleitbetriebs und für den Betrieb auf Hauptbahnen vorrangig das Betriebsverfahren mit dezentraler Fahrdienstleitung „Sicherung des Fahrens im festen Raumabstand“ angewendet. Weiterführende Informationen finden sich bei [Pachl 2004] und [Scheppan 2006].

2.5.2.1 Standardverfahren

Ein Eisenbahnbetriebsverfahren ist ein regelbasiertes System, welches mit technischen Mitteln Fahrten von Eisenbahnfahrzeugen auf Infrastrukturen zulässt. Die Klassifizierung von Betriebsverfahren ist nach der Art der Erteilung der Zustimmung zu einer Zugfahrt, durch Signalisierung oder anderweitige Aufträge, oder nach der Struktur der Fahrdienstleitung, dezentral oder zentral organisiert, umgesetzt [Lübke 2008]. Diese orthogonale Betrachtung der Betriebsverfahren ermöglicht die Unterscheidung in das bei der Deutschen Bahn AG als Standardverfahren nach Richtlinie 408 [RIL 408] – mit der Zustimmung zur Zugfahrt über Signale und einer dezentralen Fahrdienstleitung – bezeichnete Verfahren und dem Zugleitbetrieb – mit mündlichen oder schriftlichen Aufträgen zur Zugfahrt und zentraler Fahrdienstleitung.

Historisch gewachsen wird das Standardverfahren mit aktuell im Regelbetrieb am häufigsten angewendet. Durch den Einsatz von elektronischen Stellwerken wird an den Betriebsstellen zukünftig das Personal durch Technik ersetzt und der Betrieb wie vorher mit einer dezentralen Fahrdienstleitung durchgeführt. Umgangssprachlich wird die Bezeichnung „Zugmeldeverfahren“ für die Betriebsweise der Zugfolgeregelung durch Zugmeldungen und blocktechnische Sicherungsausrüstung verwendet. Das Verfahren wird auf allen Strecken in gleicher Weise angewendet, auf denen kein Zugleitbetrieb (auch signalisierter) oder ferngesteuerter Betrieb stattfindet [Pachl 2004-1].

Zur Unterscheidung zwischen dem Standardverfahren und dem Zugleitbetrieb, wird nachfolgend der umgangssprachliche Begriff „Zugmeldeverfahren“ verwendet.

Auf Hauptbahnen wird in Deutschland das Zugmeldeverfahren als Fahren im festen Raumabstand mit Streckenblockabschnitten angewendet. Die Zugfolge wird dadurch geregelt, dass die Strecke in Blöcke (Ortungsabschnitte) unterteilt wird, die jeweils nur von einem Zug zeitgleich befahren werden dürfen. Die Freigabe zur Befahrung der einzelnen Blockabschnitte erfolgt durch eine technisch signalisierte Informationsübertragung durch den Fahrdienstleiter in den zugehörigen Zugmeldestellen. Die Bahnhöfe sind durch Ein- und Ausfahrsignale sowie durch Bahnhofsteile mit Hilfe von Zwischensignalen unterteilt. Auf der freien Strecke zwischen den Bahnhöfen werden in der Regel Blocksignale zur Unterteilung der Blöcke aufgestellt. Zwischen den Fahrdienstleitern der Zugmeldestellen wird nach geregelten Vorgaben die Zugfolge abgestimmt. Durch technische Sicherung werden die Fahrdienstleiter insoweit unterstützt, dass sie jeweils nur der Fahrt eines Zuges pro Block zustimmen können [Naumann/Pachl 2004].

Dieses Verfahren ermöglicht die größte Sicherheit bei den Betriebsverfahren, ist jedoch durch den technischen Sicherungsaufwand und des zum Teil noch großen Personalbedarfs sehr kostenintensiv. Aus diesem Grund ist dieses Verfahren auf Strecken mit geringer Verkehrsleistung wirtschaftlich nur bedingt vertretbar. Mit zunehmender Automatisierung in Verbindung mit der Zentralisierung der Steuerung von Sicherungssystemen werden Möglichkeiten geschaffen, die zukünftig auch die Wirtschaftlichkeit wenig befahrener Strecken bei einem hohen Sicherheitsniveau gewährleisten [Pachl 2005], [Lenz 1999].

Bild 2.13 zeigt schematisch die Freigabe eines Blockabschnitts beim Standardverfahren in Form der signalisierten Zustimmung des Fahrdienstleiters zur Zugfahrt. Eine direkte Sprachkommunikation zwischen dem Fahrdienstleiter und dem Eisenbahnfahrzeugführer erfolgt hier nur in der Rückfallebene.

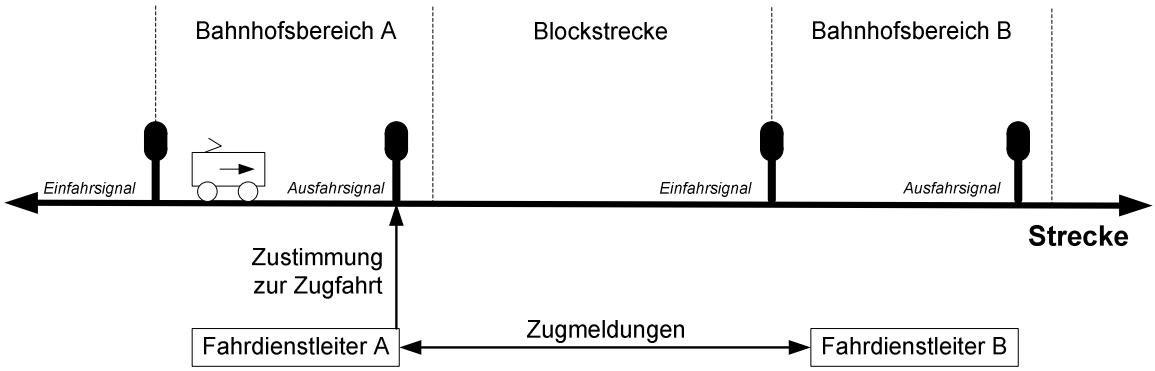

Bild 2.13: Standard- (bzw. Zugmeldeverfahren) mit Streckenblock

2.5.2.2 Zugleitbetrieb

In der Historie wurde der Zugleitbetrieb (ZLB) häufig auch als „vereinfachter Nebenbahndienst“ bei der ehem. Deutschen Reichsbahn bezeichnet. Die Sicherung der Zugfahrten erfolgt beim Zugleitbetrieb primär auf Basis von Meldungen durch und zwischen Zugleiter und Eisenbahnfahrzeugführer. Der Zugleiter überwacht von einem zentralen Arbeitsplatz aus die gewünschten Fahrstraßen und erteilt fernmündlich Fahrtfreigaben bis zu den nächsten Halteorten an den Eisenbahnfahrzeugführer. Der jeweilige Eisenbahnfahrzeug- bzw. auch der Zugführer fordern dementsprechend nach Erreichen der jeweiligen Fahrtziele weiterführende Fahrtaufträge an. Da dieses Verfahren nicht durch ein übergeordnetes Sicherungssystem überwacht wird, ist menschliches Versagen nur bedingt durch Vorgaben und Handlungsanweisungen auszuschließen. Aus diesem Grund ist das Verfahren auch nur für einfache betriebliche Verhältnisse einzusetzen [RIL 436].

Zugleitbetrieb	Merkmale	Besonderheiten
Reisezugverkehr	Betriebsprogramm	Max. 1 Stunden-Takt
Güterverkehr	Geringer Verkehr	In Taktlücken oder außerhalb der Betriebszeit des Reisezugverkehrs
Streckenhöchstgeschwindigkeit	80 km/h	

Bild 2.14: Merkmale des ZLB nach [Scheppan 2006].

Bild 2.15 zeigt schematisch die Informationsbereitstellung der Fahrzeugposition (Zuglaufmeldung) durch den Eisenbahnfahrzeugführer in Verbindung mit der Fahranfrage sowie die Erteilung der Fahrerlaubnis durch den Zugleiter beim Zugleitbetrieb.

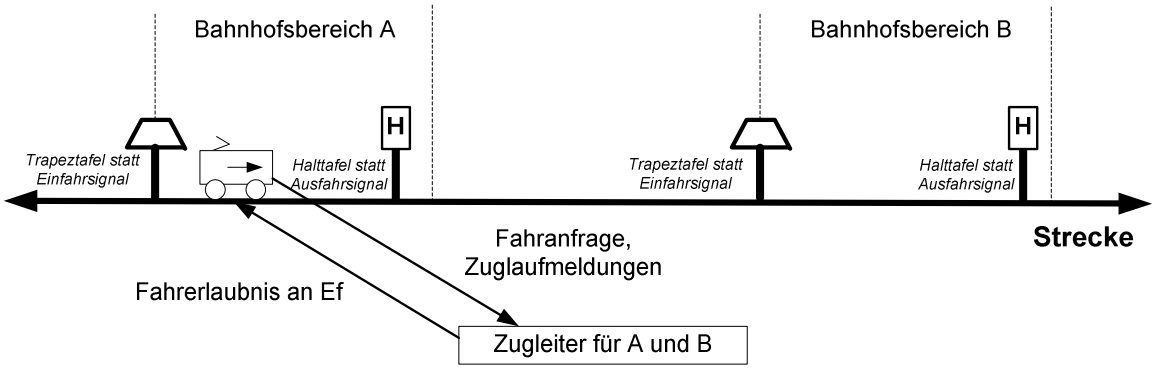

Bild 2.15: Skizze der Informationswege im ZLB

Eine Besonderheit des ZLB ist der signalisierte Zugleitbetrieb (SZB), bei dem der klassische Zugleitbetrieb durch technische Block- und Fahrstraßensicherung unterstützt wird. Auf der freien Strecke ist ein selbsttätiger Streckenblock mit zusätzlichen Streckenfreimeldeanlagen realisiert, wodurch die Streckenhöchstgeschwindigkeit auf 100 km/h heraufgesetzt werden kann. Die Ortung der Züge erfolgt entsprechend dem Standardverfahren z.B. über Achszähler.

3 ORTUNG IM SCHIENENVERKEHR

Als Ortung wird die zeitgenaue Positionsbestimmung eines sich bewegenden oder ortsfesten Objekts bezeichnet. Die Position umschreibt dabei den zeitbehafteten Aufenthaltsort des Objekts in einem Bezugs-Koordinatensystem. Für den Schienenverkehr heißt das, dass die Schienenfahrzeuge die Objekte im Transportprozess darstellen, die sich auf einer Infrastruktur bewegen. Für die Positionsbestimmung des Fahrzeugs werden Sensoren benötigt, die neben der Fahrzeugbewegung auch Bezugspunkte auf der Infrastruktur ermitteln können [Schnieder 2007]. Im dezentral organisierten System des Straßenverkehrs ist die Satellitennavigation weit verbreitet, der sich als Basisfunktion der Ortung bedient. Die Anwendung ist hierbei auf den individuellen Ersatz von Straßenkarten gerichtet. Im zentralen Schienenverkehrssystem hingegen benötigt das Betriebsleit- und Sicherungssystem insbesondere Ortungsinformationen, welche zur Lösung der spezifischen Aufgaben verwendet werden [Bikker 1998], [Poliak 2009].

3.1 Funktionen und Technologien

Im Schienenverkehr wird die Ortung diskret als verteiltes funktionales Systemmodul im Gesamtsystemzusammenhang realisiert, welches aktuell vornehmlich durch streckenseitige Sensoren aufgebaut ist. Die Ortungsinformationen werden an die Betriebsleittechnik transferiert und dem Sicherungssystem als Grundlage zur Verfügung gestellt. Bedingt durch das Fahren im festen Raumabstand dürfen Blockabschnitte nur mit jeweils einem Zug zeitgleich in einer Richtung befahren werden, wodurch die Ortungsinformation des Zuges hier hinreichend „blockgenau“ an die Betriebsleit- und -sicherungstechnik übertragen wird. Als Besonderheit im Schienenverkehr muss neben der eindimensionalen Information der Fahrzeugposition auch die Zugintegrität als zusätzliche Information erstellt werden, woraus Zugspitzen- und Zugschlussortung bzw. Zugintegritätsprüfung resultieren [Six 1996].

Durch die innovative Verlagerung der Ortungsfunktion – autark auf die Fahrzeugseite – kann je nach verwendeten Sensoren und in Verbindung mit einer Kontinuität der Information die Genauigkeit der Ortungsinformation verbessert und somit die Leistungsfähigkeit des Gesamtsystems erhöht werden. Fahrzeugseitig lässt sich auch die Zugintegrität kontinuierlich überprüfen.

Als zentrales Element der Sicherheit gilt im Schienenverkehr die Zugsicherung. Bild 3.1 stellt das System der Zugsicherung im Zusammenhang mit den relevanten Systemkomponenten dar. Deutlich wird die Gegenüberstellung der streckenseitigen Systemkomponenten der diskreten Ortung mit den fahrzeugseitigen der kontinuierlichen Ortung und der Zugintegritätsprüfung.

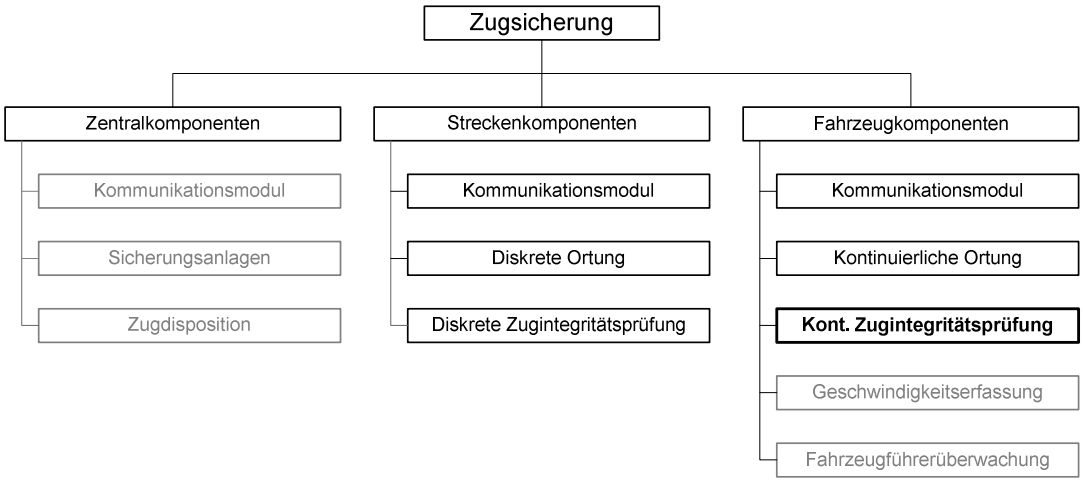

Bild 3.1: Potenzielle Systemkomponenten des Systems „Zugsicherung“

3.1.1 Funktionen der Ortung

Ortung ist immer dann erforderlich, wenn „ein bewegtes Objekt von einem Start- zu einem Zielpunkt vorbei an Hindernissen sicher und optimal geführt werden soll“. Im spurgebundenen Verkehr fällt diese Aufgabe der Führung bzw. Sicherung und Steuerung zu, welche auf der Ortung basieren. Zur Abwicklung einer Zugfahrt ist somit die Kenntnis der jeweiligen Position des Zuges verbunden mit der Zugintegrität relativ zum Fahrweg erforderlich. Dazu sind die räumlichen Verhältnisse von Referenzpunkten am Zug zu einem oder mehreren ortsfesten Referenzpunkten zu bestimmen. Der Ortungsvorgang besteht aus zwei Aufgaben, wobei zunächst die Position der Fahrzeugspitze und der Fahrtrichtung relativ zum Fahrweg bestimmt und anschließend der physikalische Fahrzeugzustand mit Erfassung der Geschwindigkeit und Beschleunigung ermittelt werden muss [Leinhos 1996].

Für einen zukünftigen, leistungsfähigen und sicheren Eisenbahnbetrieb ist eine kontinuierliche Ortung des Fahrzeugs erforderlich, die als Basis für die zeitgerechte Umstellung von Weichen, die eindeutige Übertragung von Zustimmungen zu Zugfahrten sowie für sichere Streckenbelegungsinformationen herangezogen werden kann. Die Fahrtrichtung des Zuges und die genaue Information über das jeweils befahrene Gleis (Gleisselektivität), Geschwindigkeit und Beschleunigung sowie eine Fahrt- und Stillstandsüberwachung in Verbindung mit der Zugintegritätsprüfung stellen die erforderlichen Informationsparameter für einen innovativen Bahnbetrieb dar.

Bild 3.2 zeigt im Zusammenhang die Funktionen der Ortung unabhängig von einer möglichen Realisierung. Zusätzlich werden sie im Bild den Aufgaben der Sicherungs- und Steuerungstechnik

gegenübergestellt und zugeordnet. Neben der Positionsinformation können Ortungsinformationen auch die Bestimmung der Fahrtrichtung beinhalten. Ebenfalls wird in Bild 3.2 nach sicherer und nicht sicherer Ortungsinformation unterschieden, wodurch die Relevanz einer Sicherheitsuntersuchung unterstrichen wird.

			Ortungsfunktion										
			Feststellen / Identität				**Bestimmung**				**Erkennung**		
							Position		Fahrtrichtung				
Sichere Information erforderlich			Gleisfeldelement	Fahrwegabschnitt	Fahrzeug	Zugbildung	Zugspitze	Zugschluss (Zugintegrität)	Fahrzeugseitig	Fahrwegseitig	Geschwindigkeit	Stillstand	Beschleunigung
Nicht sichere Information erforderlich													
Aufgaben der Betriebsleit- und -sicherungstechnik	**Steuerung von Zugfahrten**	Betriebsmittel disponieren	-	+	+	+	+	+	-	+	-	-	-
		Fahrprofil bestimmen	-	+	-	+	+	+	-	+	-	-	-
		Fahrbefehl ermitteln	-	-	-	+	+	+	+	+	-	-	-
		Regelung der Dynamik	-	-	+	+	-	-	+	-	+	+	+
		Stellbefehl ermitteln	-	+	-	+	-	-	+	-	-	-	-
		Fahrwegbildung	+	+	-	-	-	-	-	-	-	-	-
		Fahrwegauflösung	+	+	+	+	+	+	-	+	-	-	-
	Sicherung von Zugfahrten	Abstandssicherung	-	+	-	+	+	+	-	+	+	-	+
		Vollständigkeits-überwachung	-	-	-	+	+	+	-	-	-	-	-
		Geschwindigkeits-überwachung	-	+	-	+	+	+	-	-	+	+	-
		Bremswegüberwachung	-	+	-	+	+	-	-	+	+	-	+
		Stillstandsüberwachung	-	-	-	+	-	-	+	-	+	+	-
		Fahrwegverschluss	+	+	+	+	+	+	-	-	-	-	-
		Fahrwegüberwachung	+	+	-	-	-	-	-	-	-	-	-

Bild 3.2: Ortungsfunktionen für die Betriebsleittechnik (BLT), vgl. [Leinhos 1996]

3.1.2 Fahrzeugautarke Ortung

Die fahrzeugautarke Ortung als Basis für die Sicherungstechnik im Schienenverkehr bietet gegenüber den konventionellen streckenseitigen Einrichtungen Vorteile aufgrund der kontinuierlichen und ortsgenauen Informationsverfügbarkeit. Streckenseitige Einrichtungen haben in der Regel einen hohen Instandhaltungsaufwand, der mit hohen Personalkosten und zeitlichem Aufwand einhergeht. Zusätzlich können technologische Innovationen nur erschwert umgesetzt werden, da die Strecken selbst lange Lebensdauern aufweisen und Migration in der Regel nur in Verbindung mit einer Streckensanierung umgesetzt wird. Ein weiterer Aspekt ist der Einfluss von außen, z.B. durch Vandalismus, dem streckenseitige Einrichtungen ausgesetzt sein können. Für moderne Leit- und Zugsicherungssysteme mit einer großen erforderlichen Streckenleistungsfähigkeit, wie z.B. ETCS im Level 3 [Meyer zu Hörste 2004], ist die derzeit erreichbare Genauigkeit der Ortung, mit Ausnahme des infrastrukturseitig ausrüstungsintensiven Systems der Linienzugbeeinflussung (LZB) [Pachl 2004], nicht ausreichend. Eine kontinuierliche fahrzeugseitige Ortung mit Zugintegritätsprüfung bei hoher Genauigkeit und Verfügbarkeit, wodurch auch sicherheitsrelevante Anwendungen realisiert werden können, wird daher für die Zukunft erforderlich [Becker/Schnieder 2004], [Schnieder/Barbu 2009].

Die technischen Einrichtungen werden bei der fahrzeugautarken Ortung auf die Fahrzeuge – die produktiven Elemente – verlagert. Dadurch kann der erforderliche Instandhaltungsaufwand erheblich verringert werden, da die Instandhaltung der Ortungstechnologie beim regulären Instandhalten der Fahrzeuge mit durchgeführt werden kann. Ergänzend können dadurch Neuerungen schneller migriert und umgesetzt werden. Ein weiterer Vorteil liegt in der Verringerung der Komplexität. Durch die Vereinheitlichung der Infrastruktur können schnell und effizient neue Märkte erschlossen werden. Außerdem können auch hier Kosten eingespart werden, da weniger Aufwendungen für die Infrastruktur erforderlich sind. Hinzu kommt der Aspekt, dass mit fahrzeugautarker Ortung die für ETCS (Level 3) nötigen Anforderungen leichter erfüllt werden können. Die innovativen fahrzeugseitigen Systeme bieten ein hohes Maß an Genauigkeit, Sicherheit und Zuverlässigkeit, wodurch Sicherungssysteme gestärkt werden können. Das hat den entscheidenden Vorteil, dass die Streckenleistungsfähigkeit der Nebenbahnen mit Hilfe eines kostengünstigen und sicheren Systems gesteigert werden kann. Streckenseitige Datentransferleitungen zu Balisen, Achszählern, Signalen etc. können durch fahrzeugautarke Systeme um bis zu 80 % reduziert werden [LOCOPROL 2005]. Die Übertragung der Informationen zwischen dem Fahrzeug und einer zentralen Steuerungsebene erfolgt per Funk. Diese Art der Datenübertragung ist bei der modernen Eisenbahn durch den nahezu flächendeckenden Einsatz von GSM-R bereits realisiert. Ein Ansatz für fahrzeugbasierte Ortungsmethoden ist die satellitenbasierte Ortung. Im folgenden Abschnitt wird dieser Ansatz näher beleuchtet [Klinge 1997].

3.1.3 Satellitenbasierte Ortung

Mit Hilfe von globalen Satellitennavigationssystemen (GNSS) zur absoluten Ortung ist die Positionsbestimmung eines Objekts mittels des Prinzips der Laufzeitdifferenz möglich, indem die Position eines mit einem GNSS-Empfänger ausgestatteten Objekts – in diesem Fall eines Schienenfahrzeugs – bestimmt werden kann, sofern ausreichend Satellitensignale empfangen werden. Geschwindigkeiten und ggf. Beschleunigungen des Fahrzeugs werden ebenfalls ermittelt, wenn mindestens vier Satellitensignale empfangen werden [Gu 2005]. Bei der Eisenbahn finden die angeführten fahrzeugseitigen Informationen aktuell für Fahrgastinformationssysteme, Ladungsverfolgung im Güterverkehr sowie für dispositive Aufgaben der übergeordneten Transportleitzentralen im nicht sicherheitsrelevanten Bereich Anwendung. Sicherheitsrelevante Anwendungen mittels satellitengestützter Positionsinformation werden bei den Bahnen aktuell kaum eingesetzt [Poliak 2009], [Stadlmann 2008].

Abschattungen in Ballungsgebieten, tiefen Einschnitten oder Tunnel führen zum Verlust der satellitengestützten Positionsinformation, wodurch der Zug nicht detektiert werden kann. Der so genannte Mehrwegeeffekt führt dazu, dass Signalinformationen an Objekten reflektiert und durch Überlagerung mehrerer Signale verfälscht werden. Auch die Störanfälligkeit durch Einflüsse der EMV ist zu berücksichtigen. Positionsbestimmungen können ggf. nicht mehr eindeutig realisiert werden. Die erreichbare Genauigkeit der satellitenbasierten Ortung liegt bei etwa 10,0 m (GPS-Ortung im zivilen Bereich [Poliak 2009]), wodurch eine gleisselektive Positionsbestimmung, bei Gleisabständen – von Gleismitte zu Gleismitte – von minimal 3,5 m (bei Neubauten 4,0 m) [EBO 2008], ohne ergänzende Ortungsinformation durch weitere Sensoren kaum realisierbar ist.

Erhebliche Vorteile der satellitenbasierten Ortung sind in der vernachlässigbaren streckenseitigen Ausrüstung zu sehen, wodurch sich die bereits genannte Wartungs- und Betriebskosten reduzieren. Aufgrund der absoluten Ortung sind streckenseitige Kalibrierungen der Genauigkeit zu vernachlässigen, überdies ist diese Ortung witterungsunabhängig [Marais et al. 2003].

3.1.4 Zugortung

Die eigentliche Position eines Zuges, die als Wagenzuglänge in Deutschland eine Ausdehnung von 700 m (Fahrdienstvorschrift der DB AG Modul 408.0711) [RIL 408] haben kann, wird als punktuelle Ortungsinformation an der Zugspitze streckenseitig geortet. Verbreitet eingesetzte Systeme und Verfahren der Zug(spitzen)ortung im Schienenverkehr sind aktuell:

- Gleisstromkreise
- Tonfrequenz-Gleisstromkreise
- Achszähler mit Achszählrechnern
- Odometrie mit Referenzpunkten (LZB)
- Balisengruppen
- Fernmündliche Zuglaufmeldungen

Bereits gegen Ende des 19. Jahrhunderts wurde im Schienenverkehr als Ortungssensor und als Gleisfreimeldesystem der Gleisstromkreis (Bild 3.3) als Informationsmedium für einen freien oder besetzten Gleisabschnitt eingeführt. Bei der Implementierung werden die beiden Schienen des Gleisabschnittes elektrisch gegeneinander isoliert, wobei an der einen Seite des Gleisabschnittes ein Stromkreis aufgebaut wird, der an der anderen Seite durch ein Relais – verbunden den Stromkreis – schließt. Werden durch eine Fahrzeugachse oder aufgrund einer anderen technischen Störung die Schienen kurzgeschlossen, wird das Relais stromlos und fällt ab. Durch die Gleisfreimelde-einrichtung wird der Zustand „besetzt“ erkannt, so dass ein Zug gleisabschnittsgenau und ggf. vollständig geortet werden kann. Nachdem die letzte Achse den Abschnitt verlassen hat, ist der Kurzschluss aufgelöst und das Gleis wird wieder als „frei“ erkannt [Schnieder 2007].

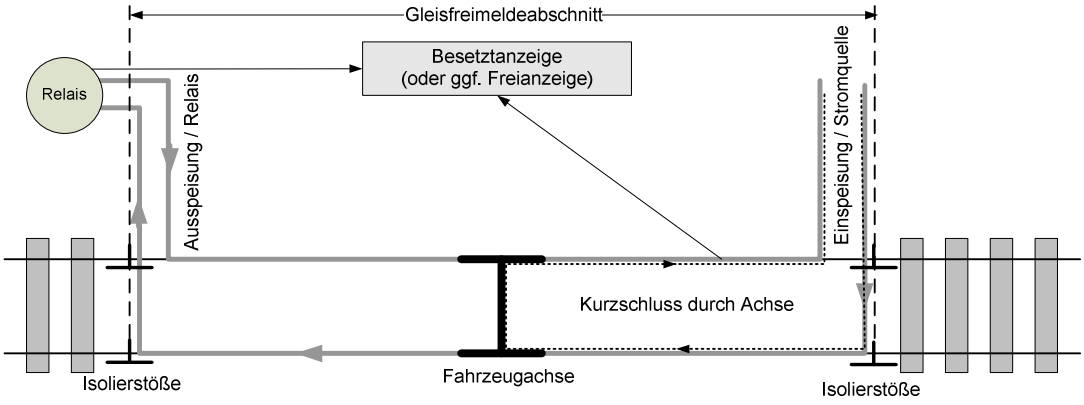

Bild 3.3: Funktionsprinzip des Gleisstromkreises

Nach einem vergleichbaren Prinzip arbeitet auch der Tonfrequenz-Gleisstromkreis (Bild 3.4). Der Schiene wird hier über einen Sender ein schwingendes Signal mit einer konstanten Frequenz zugeführt, welches auf der anderen Seite von einem Empfänger entgegengenommen wird. Eine Besetzung des Gleisfreimeldeabschnittes mit einer Fahrzeugachse führt zu einer Störung des Signals, wodurch wiederum die Gleisfreimeldeanlage den Zustand „besetzt“ erkennt und ein Zug gleisabschnittsgenau und ggf. vollständig geortet werden kann. Nachdem die letzte Achse den Abschnitt verlassen hat, ist auch die konstante Frequenz wieder beim Empfänger vorhanden und das Gleis wird ebenfalls „frei“.

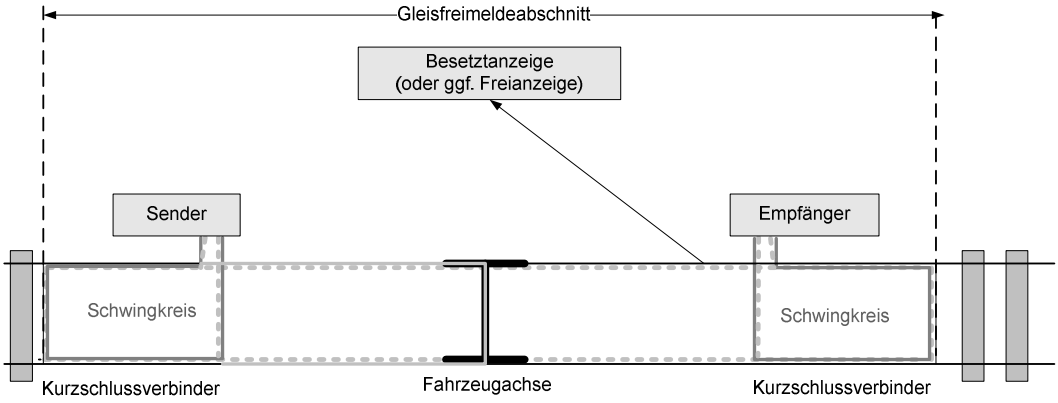

Bild 3.4: Funktionsprinzip des Tonfrequenz-Gleisstromkreises

Die gebräuchlichste Gleisfreimeldeeinrichtung ist über Achszähler und Auswerteeinheit in Form von Achszählrechnern implementiert (Bild 3.5). Ein Achszähler als streckenseitiger Sensor ist als Impulsgeber ausgeführt, der metallische Spurkränze der Fahrzeugräder durch Induktivitätsveränderung detektieren kann und die Information an ein Zählwerk weiterleitet. Bei der Einfahrt des Zuges in einen Achszählabschnitt werden die Fahrzeugachsen eingezählt, wodurch der nachfolgende Gleisabschnitt als „besetzt“ bewertet wird. Bei der Ausfahrt am nächsten Achszählpunkt werden die Achsen wieder ausgezählt. Der Gleisabschnitt wird dann als „frei“ gemeldet, wenn sich zwischen ein- und ausgezählten Achsen keine Differenz ergibt; andernfalls bleibt der Abschnitt als „besetzt“ gemeldet. Eine Isolierung der Gleise ist bei dieser Einrichtung nicht erforderlich [Schnieder 2007].

In der Regel sind an jedem Achszählpunkt zwei Sensoren dicht nebeneinander angeordnet, um zeitgleich auch die Fahrtrichtung des überfahrenden Zuges zu bestimmen.

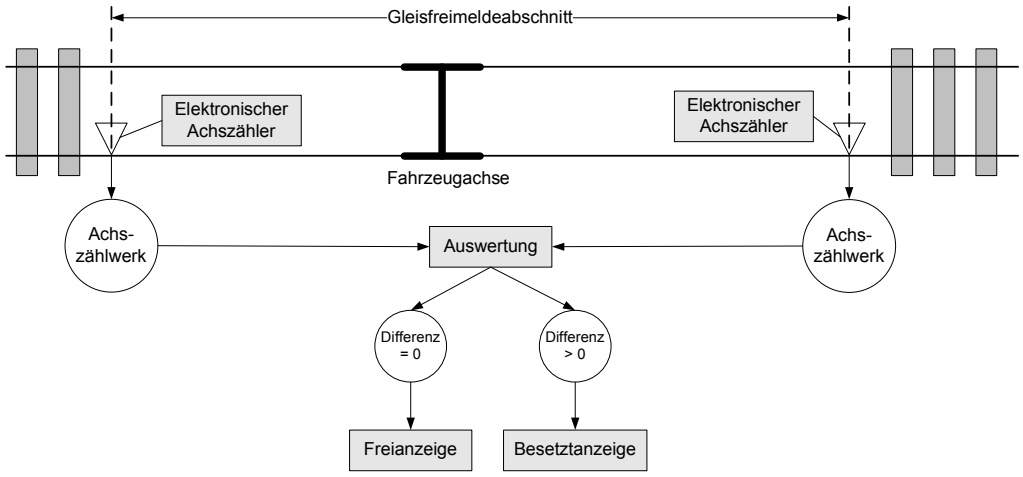

Bild 3.5: Funktionsprinzip des Achszählsystems

Eine weitere Möglichkeit der kombinierten strecken- und fahrzeugseitigen Ortung ist der Einsatz von Balisen, so genannten „elektronischen Kilometersteinen“. Diese werden als passive Elemente in

der Gleismitte in regelmäßigen Abständen installiert. Zur Umsetzung der Ortungsinformation muss das Fahrzeug mit einem Balisenlesegerät und einer digitalen Streckenkarte zur Positionsreferenzierung ausgestattet sein. Dieses Verfahren wird für das zukünftige Leit- und Sicherungssystem ETCS (European Train Control System) auf den europäischen Hauptkorridoren Anwendung finden [Meyer zu Hörste 2004].

Ein vergleichbares kombiniertes System bietet auch die Linienzugbeeinflussung (LZB), bei dem streckenseitig ein Informationsleiterkabel integriert ist, das in regelmäßigen Abständen von jeweils 100 m das fahrzeugseitige Odometersystem kalibriert und somit eine relativ genaue Ortung gewährleistet.

Als nicht technisches Verfahren wird auf Nebenbahnen größtenteils die Fahrzeugortung in Verbindung mit der Gleisfreimeldung fernmündlich zwischen dem Eisenbahnfahrzeugführer bzw. dem Zugführer und dem Zugleiter in Form einer Zugmeldung (hier Zugschlussmeldung) durchgeführt. Auch auf Strecken mit Zugmeldeverfahren erfolgt bei alter Sicherungstechnik die Gleisfreimeldung ebenfalls durch das streckenseitige Personal visuell in Verbindung mit der Kommunikation zwischen den Stellwerken.

Die angeführten streckenseitigen Einrichtungen zur Ortung der Zugspitze haben allesamt die Möglichkeit gleichzeitig auch die Zugintegrität festzustellen; allerdings kann der Zug jeweils nur diskret, d.h. beim Überfahren der jeweiligen Sensoren und dementsprechend genau in Abhängigkeit von der Entfernung zweier Sensorpunkte geortet werden, wodurch die Streckenleistungsfähigkeit beeinflusst wird. Die z. Zt. verwendeten Sensoren inkl. Eigenschaften zur Ortung werden in Bild 3.6 nachfolgend vorgestellt.

3.1.5 Zugvollständigkeitsprüfung

Neben der Ortungsinformation der Zugspitze ist im spurgebundenen Verkehr aufgrund der fahrzeugverbindenden Kupplungsstellen und der Länge der Züge auch die Information über die Zugintegrität sicherheitsrelevant. Unerkannte Zugtrennungen können zu Kollisionen führen und gefährliche betriebliche Auswirkungen nach sich ziehen. Auch muss stets nach einer gewollten Änderung der Zugzusammenstellung die „neue“ Zugvollständigkeit zuverlässig erkannt werden. Zur Steigerung der betrieblichen Leistungsfähigkeit in Verbindung mit einem innovativen Sicherungssystem ist eine kontinuierliche Ortungsinformation des Zugschlusses daher ebenso erforderlich. Bei der Ortung des Zugschlusses kann zwischen zwei dominierenden Verfahren unterschieden werden. Die Ermittlung der Zugvollständigkeit mit Hilfe der streckenseitigen Ortung wird heute flächendeckend eingesetzt.

Als alternatives Verfahren wird die Position des letzten Fahrzeugs relativ zur Position des führenden bestimmt, wobei der fahrzeugseitig gemessene Abstand zwischen den beiden Positionen als gerichtete Entfernung (E) nicht mehr als die Gesamtlänge (l) des Zuges betragen darf.

$$\left| E_{(Zugschluss-Zugspitze)} \right| \leq l_{Triebfahrzeuge} + x \cdot l_{Wageneinheit} \qquad (3.1)$$

Bedingt durch Kurvenfahrten oder im Bereich von Kehrschleifen wird die gerichtete Entfernung zwischen Zugspitze und -schluss kleiner als die reale Zuglänge.

Neben der relativ gemessenen, streckenseitig auf einzelne Strecken- und Blockabschnitte bezogenen technisch gestützten Ortungsinformation wird auf Strecken ohne technische Einrichtungen vorrangig mit fernmündlichen Zugschlussmeldungen gearbeitet, die ebenfalls streckenabschnitts-bezogen die Zugintegrität gewährleisten.

Innovative Ansätze bestehen in kombinierten Lösungen der streckenseitigen Zugspitzenortung in Verbindung mit einer fahrzeugseitigen Zugintegritätsprüfung z.B. mittels durchgängiger Bussysteme, Informations- und Steuerleitungen oder Hauptluft- und Hauptluftbehälterleitungen etc. Fahrzeugautarke Lösungen mittels GSM-R oder Satellitenunterstützung am Zugende (dem letzten Fahrzeug), die mit der Zugspitze kommunizieren, machten streckenseitige Ortungseinrichtungen überflüssig. Diesbezüglich tiefer gehende Ansätze sind in den Arbeiten von [Kupke 2007] und [Quante et al. 2000] zu finden. Eine umfassende Analyse in Verbindung mit einer Auswertung wurde in der Diplomarbeit von Gericke [Gericke 2008] zum Thema Zugvollständigkeitsprüfung vorgestellt.

Weiterführende Ansätze sind u.a. fahrzeugseitig mitzuführende Zugschlusssender, die über streckenseitige Transponder die Zugvollständigkeit übermitteln; dieses System wird bei der Osthannoversche Eisenbahnen AG angewendet. Aber auch kombinierte Systeme mit fahrzeug-seitigen Sendern und infrastrukturseitigen Gleisschaltmitteln zur Zugerkennung werden vorwiegend bei S- oder Straßenbahnen eingesetzt.

3.1.6 Anforderungen

An die Ortungsinformation im Eisenbahnbetrieb werden im Vergleich zum Straßenverkehr weitaus höhere Anforderungen gestellt. Eine hohe Sicherheitsrelevanz besteht, seitdem Ortsinformationen von Zügen für die Gleisfreimeldung in Verbindung mit Streckenfreigaben für nachfolgende Züge eingesetzt werden. Entsprechend der Eisenbahn-Bau- und Betriebsordnung beträgt der Gleismittenabstand (gemessen zwischen den Mittelachsen zweier paralleler Gleise) mindestens 4 m, wodurch ersichtlich wird, dass für eine gleisselektive Ortung eine Querabweichung von < 2 m nicht überschritten werden darf [Hartwig et al. 2005]. Im Zusammenhang mit der Einführung von ETCS werden auch detaillierte Anforderungen an die Genauigkeit der Ortung gestellt, wobei für die Ortungsinformation mittels streckenseitiger Balisen in Verbindung mit der fahrzeugseitigen Einrichtung eine geforderte Längsgenauigkeit von 5 m +/- 2 % besteht. Basierend auf der eindeutigen Zuordnung der streckenseitigen Komponenten kann die Gleisselektivität gewährleistet werden [DemoORT 2007], [Geistler/Böhringer 2004].

Bei einer fahrzeugautarken Ortung mit satellitenbasiertem Teilsystem ohne streckenseitige Zusatzinformationen besteht grundsätzlich das Problem der Querabweichung zur gleisbezogenen Fahrtroute eines Zuges. Zur Bestimmung einer genauen Position sind im Normalfall mindestens vier Satellitensignale erforderlich. Durch Abschattungseffekte oder Mehrwegeausbreitung kann es zu ungenauen Messergebnissen bis hin zum Signalabriss kommen, was insbesondere für die

sicherheitsrelevante Ortung eine erhebliche Einschränkung auch in Bezug auf die Verfügbarkeit darstellt. Zur Erhöhung von Genauigkeit und Verfügbarkeit einer satellitenbasierten Ortungseinrichtung mit Sicherheitsrelevanz ist die Datenfusion mit Informationen weiterer Sensoren bzw. Teilsysteme erforderlich.

Dafür können u.a. Sensoren herangezogen werden [Klinge 1997], [Hartwig et al. 2005]:

- Odometer (Kilometerzähler)
- Balisen / Induktionsspulen / Gleismagnete
- Inertial-Systeme
- Wirbelstromsensoren
- Radar
- GSM-R

Sie erhöhen als zusätzliche Stützsensoren die Ortungsverfügbarkeit, sofern eine GNSS-basierte Positionsbestimmung nicht exakt genug oder kurzfristig ausgefallen ist. Ergänzend kann die Integrität der Ortung stark verbessert werden, da die Ergebnisse der unterschiedlichen Systeme gegeneinander geprüft werden können [Gu 2005].

Aufgrund der vorgegebenen Trajektorie des Fahrweges im Schienenverkehr sind die für Ortungseinrichtungen relevanten Freiheitsgrade auf die Längsrichtung beschränkt. Die Streckenverläufe können mittels digitaler Streckenkarten in Systeme integriert (vgl. ETCS) und anschließend Abweichungen der Messergebnisse zum tatsächlichen Aufenthaltsort durch das Verfahren des „Map-Matchings“ bestimmt werden [DemoORT 2007]. Unregelmäßigkeiten bei der Auswertung der Längsrichtung können ggf. schwer erkannt werden, auch stellt die digitale Streckenkarte aufgrund der stets erforderlichen Aktualität ein gewisses Fehlerpotenzial dar [Poliak 2009].

3.2 Ortungssensoren

Zur Realisierung von strecken- und fahrzeugseitiger Ortung wurde eine Reihe von Sensoren in den vorhergehenden Abschnitten angeführt. Neben Gleisstromkreisen, Tonfrequenz-Gleisstromkreisen und Achszählern für streckenbasierte Systeme wurden GNSS (Global Navigation Satellite System) sowie die digitale Streckenkarte für fahrzeugseitige Systeme vorgestellt. Ergänzend für dazu bestehen noch Wirbelstromsensoren, Doppler-Radar und Odometer. Häufig werden fahrzeugseitig Odometer in Ergänzung mit fahrwegseitigen Referenzpunkten – wie beispielsweise beim System der Linienzugbeeinflussung (LZB), bei Zugschlusssendern mit zugschlussreagierenden Kontakten oder dem Einsatz von Balisen – für Wegmessungen eingesetzt, wobei Nachteile bei der Messgenauigkeit durch Gleiten oder Schleudern der angetriebenen Fahrzeugachse auftreten können, an die das Odometer angeschlossenen ist. Eine Verwendung in einem hochgenauen, sicherheitsrelevanten Ortungssystem wird dadurch eingeschränkt. Eine detaillierte Übersicht über Sensoren sowie deren Aufbau und Anwendungsmöglichkeiten ist in [Schnieder 2007] aufgeführt.

Unter Berücksichtigung der genannten Quelle wurde Bild 3.6 abgeleitet, das die Leistungsfähigkeit der Sensoren in Bezug zu einem jeweiligen Ortungssystem vergleichend zeigt.

Die mit x gekennzeichneten Zuordnungen sind uneingeschränkt vorhanden, mit (x) nur mit Einschränkung. Die Kennzeichnung --- bedeutet, dass keine Einflüsse vorhanden sind.

	Achszähler/ Achszählkreis	Gleisstromkreis	Balise/ Transponder	Wirbelstromsensor	Odometer	GNSS-basiertes System	Doppler-Radar	Digitale Karte mit Algorithmus
Vorliegende Ortsinformation:								
absolut	(x)	x	x	(x)		x		x
relativ				x	x		x	
punktförmig	(x)		x					
kontinuierlich				x	x	x	x	x
abschnittsweise	x	x	x					
Signaltechnisch sicher:	x	x	x		x			x
Einschränkung der Ortungsgenauigkeit durch:								
Signalabschattung	---	---	---	---	---	x	(x)	---
Elektromagnetische Einflüsse	x	x	---	x	---	x	x	---
Raddurchmesser	x	---	---	---	x	---	---	---
Witterungseinflüsse	(x)	x	---	---	---	x	(x)	---
Schlupf	---	---	---	---	x	---	---	---
Fahrgeschwindigkeit	(x)	---	x	(x)	---	---	x	---
Informationsübertragung auf das Fahrzeug:								
Sender – Empfänger Funksignale			x			x		
Fahrzeugseitige Signalgenerierung			x	x	x		x	
Externe / Streckenseitige Signalgenerierung	x	x	(x)			(x)		x
Informationsübertragung an Verarbeitungssystem:								
Streckenseitige Kabelverbindungen	x	x	(x)					
GSM-R durch Triebfahrzeug			x	x	x	x	x	x
Systemintegration:								
streckenseitig	x	x	x					
fahrzeugseitig				x	x	x	x	x

Bild 3.6: Eigenschaften der Ortungssensoren

Mit Hilfe der tabellarischen Sensorübersicht lassen sich Aussagen über die Potenziale für den Einsatz in einem innovativen, fahrzeugautarken Ortungssystem ableiten.

3.3 Zukunftsweisende Zugortung

Zur Realisierung von fahrzeugautarker Ortung gibt es eine Vielzahl innovativer Ansätze und Ideen. Grundlage der meisten Ansätze ist die satellitengestützte Ortung. Insbesondere für den Einsatz im sicherheitsrelevanten Bereich reicht diese als alleinige Eingangsortsinformation nicht aus, da Abschattungseffekte in Tunnel, in bebauten Gebieten usw. eine kontinuierlich verlässliche Ortungsinformation behindern. Auch eine gleisgenaue Positionsermittlung ist mit der reinen satellitenbasierten Ortung nicht möglich. Aus diesen Gründen ist eine Fusion mehrerer verschieden sensierter Informationen erforderlich. Bild 3.7 zeigt die schematische Darstellung eines innovativen Ortungssystems für sicherheitsrelevante Anwendungen. Zentraler Kern des Systems ist ein Modul, in dem die von verschiedenen Sensoren ermittelten Ortungsinformationen in Form von Sensorsignalen zusammengeführt werden, so dass aus mindestens drei eigenständig nicht sicheren Informationen eine sichere Positionsinformation generiert werden kann. Bestandteile der sicherheitsrelevanten Information können neben der genauen Position auch Geschwindigkeits- und Beschleunigungsinformationen sein. Mit Hilfe der genauen Ortungsinformation können sicherheitsrelevante Systeme – wie Zugsicherungssysteme in Verbindung mit Betriebsverfahren – leistungsfähiger gestaltet werden, wobei eine weitere Voraussetzung die verlässliche und sichere fahrzeugseitige Zugintegritätsprüfung ist [Gericke 2008], [Kupke 2007], [Leinhos 1996], [Klinge 1997].

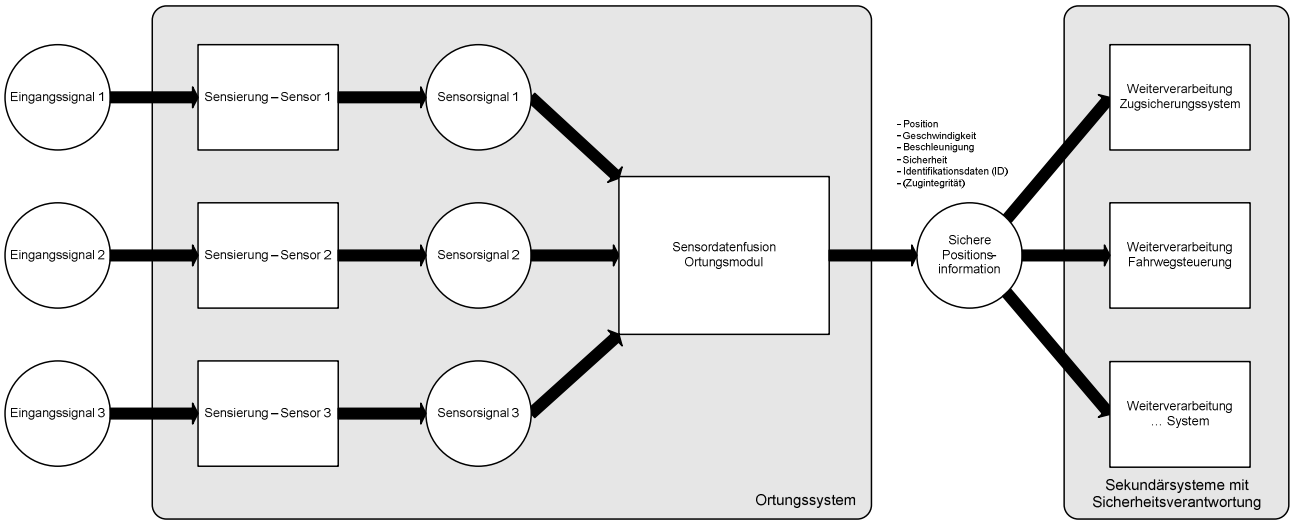

Bild 3.7: Schema der sicherheitsrelevanten Ortung mit Multisensorsystem

Zur Darstellung der schematischen und funktionalen Zusammenhänge sowie der Prozesse wurde das Beschreibungsmittel der Petrinetze verwendet. Auf tiefer gehende Informationen zum Beschreibungsmittel selbst, zu begleitenden Methoden oder auch Werkzeugen wurde in dieser Arbeit verzichtet. Weiterführende Literatur ist u.a. in [Schnieder 1999] zu finden.

Zur Realisierung einer sicherheitsrelevanten Ortungsinformation auf dem Fahrzeug selbst ist es erforderlich, entsprechend das Fahrzeug als Objekt auf der Infrastruktur in einem Referenzsystem – in der Regel einer digitalen Streckenkarte – genau zuzuordnen. Mit Hilfe des Ortungsmoduls lassen

sich nachfolgend neben der genauen und verlässlichen Position weitere Informationen wie Geschwindigkeit und Beschleunigung des Fahrzeugs, aber auch die Bewegungsrichtung und ggf. Identifikationsnummern (Zugnummern o.ä.) als Informationen für relevante Empfänger erstellen. Bild 3.8 stellt den prinzipiellen Ortungszusammenhang dar.

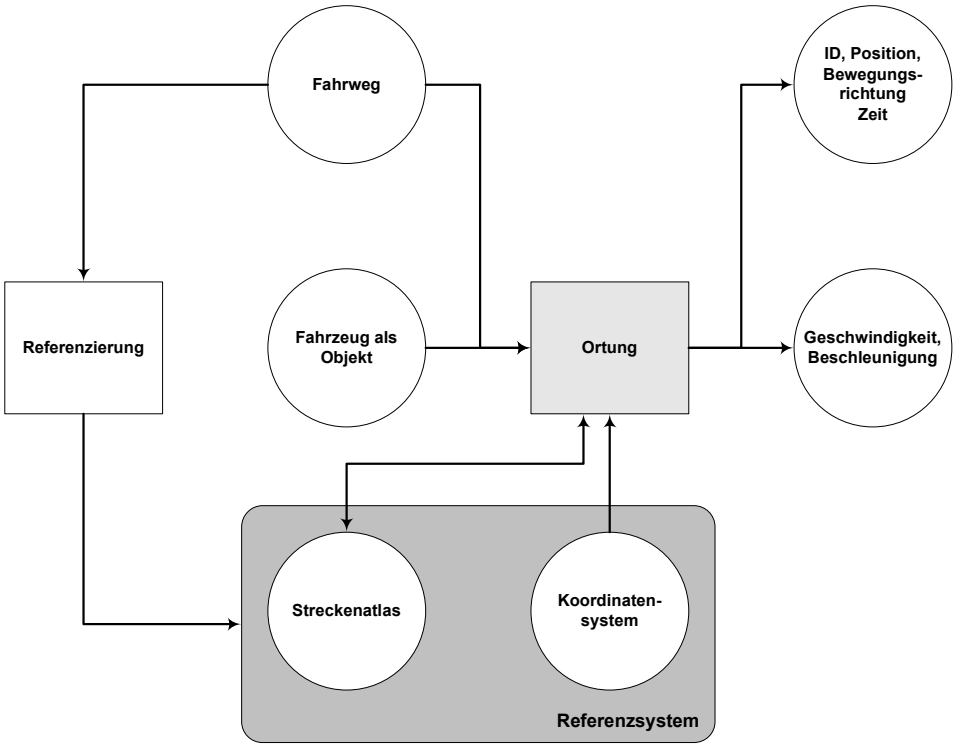

Bild 3.8: Ortungsprinzip im spurgebundenen Verkehr, nach [Leinhos 1996]

In Bild 3.9 wird das funktionale Ortungsmodul im Detail ergänzend aufgeführt und die fahrzeugautarke Zustandserfassung der Zugspitzenortung dargestellt.

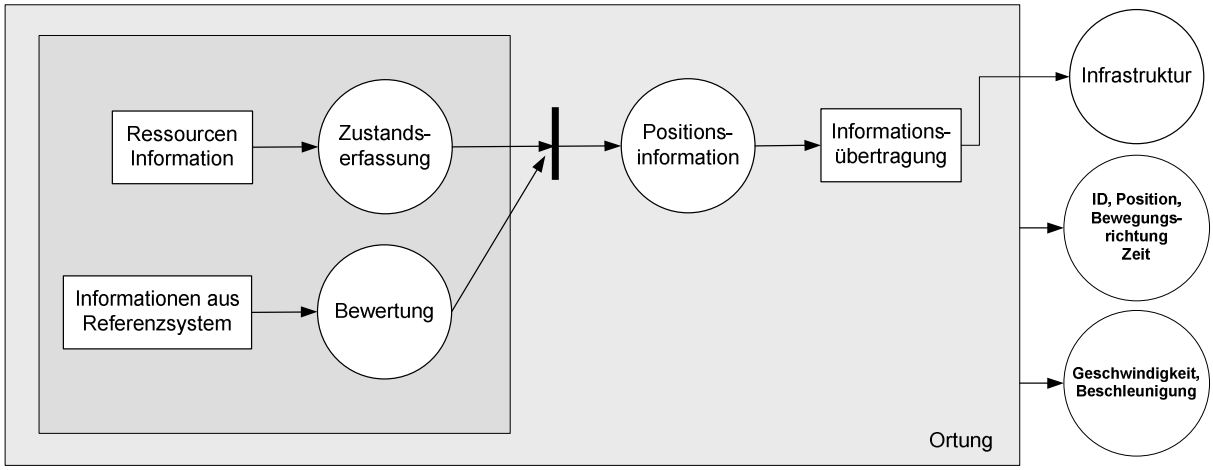

Bild 3.9: Zustandserfassung der Zugspitzenortung

3.4 Zukunftsweisende Zugintegritätsprüfung

Die verlässliche Feststellung des Zugschlusses ist ein grundlegender Bestandteil für den sicheren Schienenverkehr. Zur innovativen Leistungssteigerung ist im Zusammenhang mit der fahrzeugautarken Ortung auch eine fahrzeugseitige Prüfung der Zugintegrität zu berücksichtigen, wie sie bei ETCS im Level 3 festgeschrieben ist. Eine abschließende fahrzeugautarke Lösung für allgemeine Anwendungen existiert derzeit nicht.

In einer Vielzahl von Ansätzen wurden für diese Aufgabenstellung Lösungen entwickelt. Unter Berücksichtigung der Migrationsfähigkeit von Fahrzeugen, insbesondere im Güterverkehr zwischen altem und neuem Wagenmaterial, ist in Europa momentan als einzig verbindendes Kommunikationsmedium die durchgehende Hauptluftleitung an allen Fahrzeugen vorhanden. Mit Hilfe der durchgängig gekuppelten Hauptluftleitung wäre theoretisch eine Zugintegritätsprüfung möglich. Aufgrund weniger, trotz gekuppelter Luftleitung unerkannter Zugtrennungen in der Vergangenheit wurde dieser Ansatz als alleinige Prüfeinrichtung als unzureichend angesehen. Zur Verdeutlichung zeigt Bild 3.10 das Blockschaltbild der indirekt wirkenden Druckluftbremse im Schienenverkehr mit der durchgängigen Hauptluftleitung als Kommunikationsschnittstelle zwischen einem Triebfahrzeug und einem Wagen am Zugschluss.

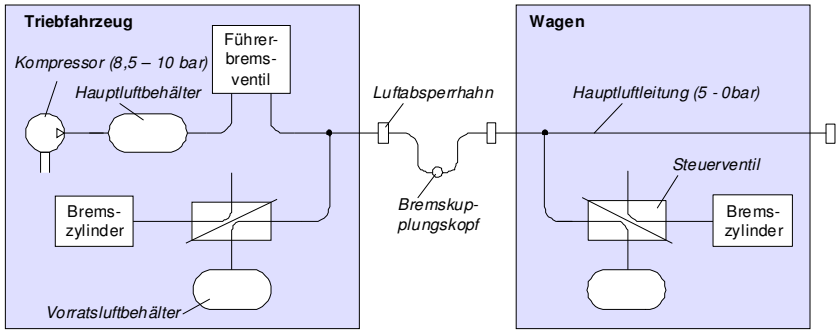

Bild 3.10: Kommunikationsschnittstelle zwischen Triebfahrzeug und Wagenzug, nach [Gralla 1999]

In derselben Form ist auch die Kommunikationsschnittstelle zwischen den einzelnen Wagen ausgeführt. Eine in [Gericke 2008] ausgeführte Recherche von europäischen und US-amerikanischen Patenten hat weitere Lösungsansätze zur fahrzeugseitigen Zugintegritätsprüfung ergeben, wobei nachfolgende Kernelemente neben der Hauptluftleitung herausgestellt wurden:

- Positionsbestimmung und/oder Geschwindigkeitsmessung über GNSS
- Zusätzliche Signalleitung (vergleichbar der Informations- und Steuerleitung bei Reisezügen)
- Ausgesendete elektromagnetische Signale
- Kraftmessungen am Zughaken des Triebfahrzeugs
- Zuginterne Funkkommunikation zwischen dem ersten und letzten Fahrzeug eines Zuges

Die grundlegende Anforderung an ein Zugintegritätsprüfungssystem ist die Zustandserfassung mit der korrekten Informationsweitergabe an ein informationsverarbeitendes System über Kommunikationsschnittstellen. Mit Hilfe von Energie-, Gesamtzug- (z.B. Länge und Gewicht) sowie Zugbewegungsmerkmalen ist eine zuverlässige Aussage über die Zugintegrität unter Berücksichtigung möglicher Fehlfunktionen zu erzielen. Das folgende Informationsflussschaubild 3.11 zeigt die erforderlichen Informationswege eines derartigen Systems auf.

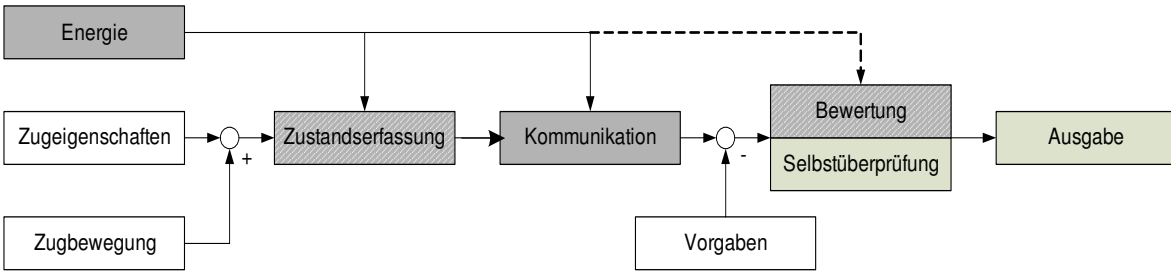

Bild 3.11: Informationsflussschaubild der Zugintegritätskontrolle

In Ergänzung zum Informationsfluss wird in Bild 3.12 das Modell des funktionalen Ortungsmoduls am Zugschluss im Detail aufgeführt und die Umsetzungsidee zur Zustandserfassung verdeutlicht.

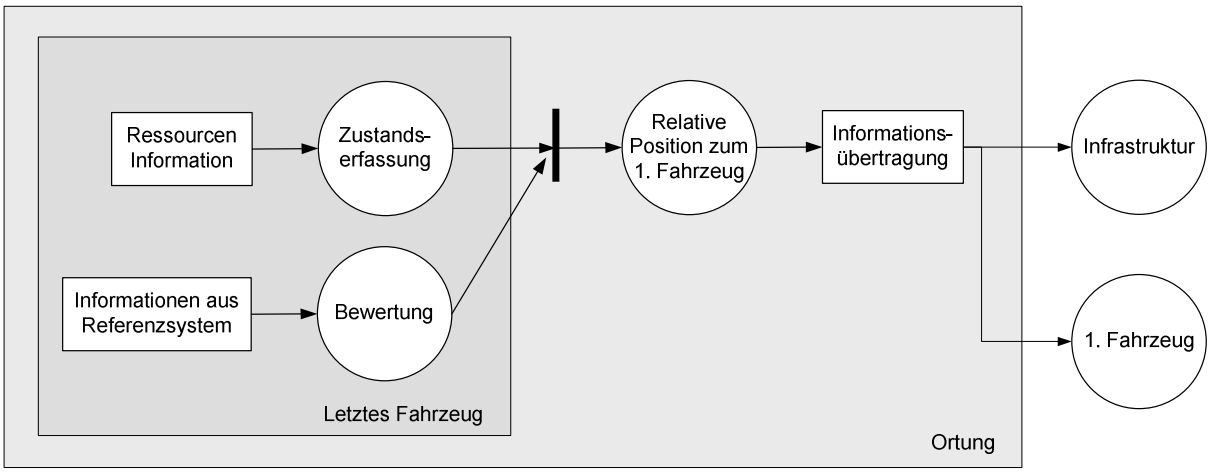

Bild 3.12: Zustandserfassung der Zugintegrität

Zur geeigneten Lösungsfindung sind die Funktionen der fahrzeugseitigen Zugintegritäts-prüfeinrichtung herauszustellen und das System funktional zur Teillösungsfindung zu dekomponieren.

Bei der allgemeinen Lösungseingrenzung für ein System zur fahrzeugautarken Zugintegritäts-prüfung ist vorrangiges Ziel, eine Lösung zu finden, die sowohl auf aufwändige Messtechnik als auch auf teure und/oder empfindliche Kommunikationsleitungen zur Signalübertragung verzichten kann [Gericke 2008]. Daher hat sich als eine vielversprechende Lösung zur Informations-übertragung der Einbezug einer durch den gesamten Zug geführten zusätzlichen Signalleitung ergeben – nicht zuletzt bezüglich der sicherheitsrelevanten Eigenschaften. Im Reisezugverkehr bereits Standard, hält die so genannte Informations- und Steuerleitung (I/S-Leitung) mittlerweile auch Einzug in neue, schnell fahrende Güterwagen, um zusätzlich Informationen zu modernen elektropneumatischen Bremssystemen bereit zu stellen und somit die Ansteuerung der einzelnen Wagenbremsen zu beschleunigen. Für die Zugintegritätsprüfeinrichtung kann ein elektrisches Signal, das vom Zugende ausgeht, über die Leitung gesendet werden, welches durch eine Auswerteeinheit auf dem Triebfahrzeug plausibilisiert wird. Im Falle einer Zugtrennung würde auch die Leitung getrennt und ein Signalausfall im Triebfahrzeug erkannt werden, wodurch eine Zwangs-bremsung ausgelöst werden würde. Weitergehende Störungen, wie z.B. Beschädigungen an der Leitung, würden ebenso erkannt werden, wodurch eine sicherheitsrelevante Integritätsprüfung nach dem „fail-safe“ Prinzip umgesetzt werden könnte. Als Energiequelle für die signaleinspeisende Ein-heit am Zugende (End of Train – EOT-Unit) kann die Hauptluftleitung, welche Druckluft enthält, dienen, wodurch zusätzlich die Zugintegrität redundant überprüft werden könnte [Theeg 2009], [Gericke 2008]. Bild 3.13 zeigt exemplarisch den schematischen Aufbau einer innovativen Zugintegritätsprüfeinrichtung.

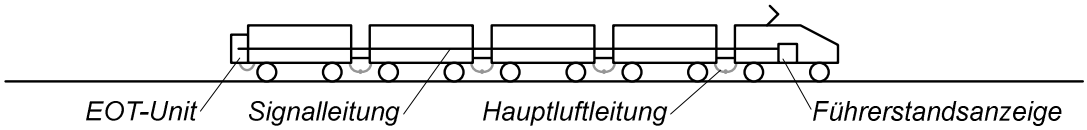

Bild 3.13: Strukturierter Lösungsansatz zur Zugintegritätsprüfung

In Verbindung mit dem im nachfolgenden Abschnitt vorgestellten System DemoORT wäre durch geeignete Kombination mit dem vorgestellten Lösungsansatz zur Zugintegritätsprüfung eine rein fahrzeugautarke Ortungseinrichtung sowohl für die Zugspitze als auch für den Zugschluss für sicherheitsrelevante Anwendungen umsetzbar. Weiterführende Ansätze zur Zugintegritätsprüfung, insbesondere mittels funkbasierter und energieautarker Kommunikation die sind u.a. auch in [Kupke 2007] zu finden.

3.5 Ausgewählte Ortungsprojekte

Einige Forschungsprojekte, welche sich allesamt auf die Basis der Satellitenortung als primäre Ortsinformation beziehen, wurden auf dem Gebiet der fahrzeugautarken Ortung bereits konkretisiert [Poliak 2009]. Dabei sind folgende Projekte zu nennen, auf die an dieser Stelle verwiesen wird:

- APOLO (Advanced Position Locator System) [Alcouffe/Barbu 2001]
- GADEROS (Galileo Demonstrator for Railway Operation System) [Urech et al. 2002]
- GEMINI (Genauigkeit satellitengestützter Bewegungsmesssysteme und Entwicklung einer Messplattform für Landfahrzeuge) [Hänsel et al. 2007]
- GEORAIL (railway geodesy guidelines for use of absolute coordinates in railway geo-referenced applications) [Barbu 2008]
- GIRASOLE (Galileo Safety of Life Receivers Developement) [Poliak 2009]
- GRAIL (GNSS Introduction in the RAIL sector) [Barbu et al. 2008]
- RAILORT (Ortung im spurgebundenen Verkehr auf der Basis von Satelliten-Navigation) [Bikker 1998]
- RUNE (Design and Demonstration of a GPS/EGNOS-Based Railway User Navigation Equipment) [Poliak 2009]
- SATNAB (Satellitennavigationsgestütztes Navigations-Bodenexperiment) [Illgen et al. 2000], [Däubler 2002]

Im Bereich der sicherheitsrelevanten Anwendungen ist in Europa aktuell nur ein GNSS-basiertes Projekt zur fahrzeugautarken Ortung in Betrieb. Eine erste Pilotanwendung ist in der Nähe von Linz (Österreich) zu finden, bei der eine Nebenbahnstrecke im Zugleitbetrieb ausgerüstet wurde [Stadlmann 2008], [Poliak 2009]. Ein weiterer theoretischer Ansatz ist in [Filip et al. 2001] zu finden.

Als Referenzierung werden nachfolgend zwei ausgewählte Projekte LOCOPROL [LOCOPROL 2005] und DemoORT [Meyer zu Hörste 2007] tiefer gehend betrachtet, da diese im Bereich der Konkretisierung für sicherheitsrelevante Anwendungen geeignet erscheinen.

3.5.1 Projekt LOCOPROL

Im Rahmen des französischen Projekts LOCOPROL (Low Cost satellite based train location system for signalling and train Protection for Low density lines) wurde ein kostengünstiges, ausfallsicheres, satellitenbasiertes und fahrzeugautarkes Ortungssystem konzipiert. Geringe Lebenszykluskosten, vorrangig die Einbindung in Sicherungssysteme von Nebenbahnen aber auch die Interoperabilität mit ETCS waren Ziele des Projekts. Durch die Verwendung von funkbasierter Datenübertragung der Ortungsinformationen werden die Kosten niedrig gehalten, wobei eine sichere Informationsübertragung zu beachten ist. Auf eine permanente Informationsübertragung zwischen dem Fahrzeug und der Infrastruktur bzw. anderen Fahrzeugen wird verzichtet.

Unter normalen Betriebsbedingungen erfolgt die Positionsbestimmung direkt über Satellitensignale, wobei keine spezifischen Integritätsanforderungen verlangt werden und die Position direkt aus dem unbearbeiteten Satellitensignal berechnet wird. Das LOCOPROL-System verwendet ergänzend zur satellitenbasierten Ortung „Stützsensoren“ für den Fall von Abschattungseffekten. Der fehlende Freiheitsgrad, die genaue Position des Zuges auf der Strecke, wird mit Hilfe des so genannten „1D-Algorithmus“ ermittelt. Die Laufzeitdifferenz, die zwischen zwei Satelliten und dem Zug gemessen wird oder die Laufzeitdifferenz, die zwischen einem Satelliten und dem Zug mit Hilfe einer synchronisierten Uhr im Zug gemessen wird, werden dabei berücksichtigt. Die ausgewerteten und berechneten Signale werden diskret und nicht kontinuierlich zur Positionsbestimmung an das Ortungsmodul übertragen [Marais et al. 2003].

Der konzeptionelle Ansatz von LOCOPROL fusioniert die Informationen der ausfallsicheren Abbildung der Strecke in einer digitalen Streckenkarte, der ausfallsicheren Verbindung der einzelnen Streckenabschnitte zu einer Gesamtstrecke als so genannte „Interlocking-Function“ sowie der multiplen eindimensionalen Satellitenortung.

In Bild 3.14 ist der Aufbau des LOCOPROL-Systems mit dem zugehörigen Datenfluss wiedergegeben.

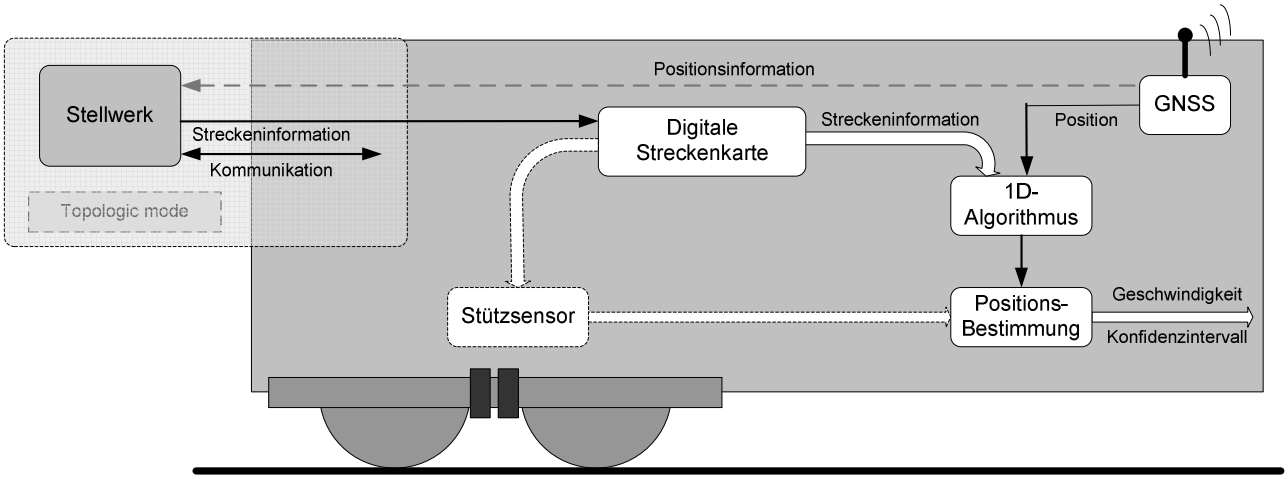

Bild 3.14: Aufbau und Datenfluss des LOCOPROL-Systems

Der LOCOPROL-Betriebsprozess wird durch zwei Betriebsarten, dem „Line Based“ (streckenbasierter Modus) und dem „Topologic“ Modus realisiert. Der „Line Based“ Modus wird eingesetzt, wenn ein Zug entlang eines Streckenabschnitts ohne Abzweigungen fährt und die Ortung des Zuges in diskreten zeitlichen Abständen erfolgen kann, da bereits zwei Freiheitsgrade vorgegeben sind.

Im „Topologic“ Modus wird an Stellen, an denen fahrzeugseitig keine zuverlässige Aussage der genauen Position mehr getroffen werden kann, z.B. an Weichen, zwischen dem Fahrzeug und der streckenseitigen Infrastruktur – den Stellwerken – ein Informationsaustausch bzgl. der Weichenstellungen durchgeführt, wodurch das System die jeweils erforderliche digitale Streckenkarte abgleichen kann, um den „Line Based“ Modus wieder aufzunehmen. Zwischen dem fahrzeugseitigen System und den streckenseitigen Stellwerken werden kontinuierlich elektronische Token ausgetauscht. Die jeweilige Strecke ist in einzelne Streckenblöcke unterteilt, die jeweils mit einem Token beaufschlagt sind. Der Zug, der einen Abschnitt befährt, muss im Besitz des zugehörigen Tokens sein, wodurch die Fahrerlaubnis realisiert wird. Dasselbe Prinzip wird auch für das Weichenmanagement eingesetzt. Nur der Zug, der im Besitz des entsprechenden Tokens ist, kann eine Fahrwegänderung anfordern. Die Informationsübertragung der Fahrerlaubnis für den Eisenbahnfahrzeugführer erfolgt über eine Führerstandsignalisierung. LOCOPROL ist ersten Demonstrationstests unterzogen und bereits auf eine Vielzahl potenzieller, sicherheitsrelevanter Anwendungsmöglichkeiten hin untersucht worden. Eine weiterführende Systemnutzung ist aber derzeit nicht umgesetzt [LOCOPROL 2005].

3.5.2 Projekt DemoORT

Im Gegensatz zum vorhergehenden Projekt wird DemoORT (Entwicklung eines Demonstrators für Ortungsaufgaben mit Sicherheitsverantwortung im Schienengüterverkehr) durch ein deutsches Konsortium bearbeitet [DemoORT 2007]. Das primäre Ziel des Projekts liegt in der Sicherheitsverantwortung des Systems für eine rein fahrzeugautarke Anwendung der Ortung. Auch in diesem Projekt ist die Einbindung in Sicherungssysteme u.a. von Nebenbahnen angestrebt, wofür Langzeittests unter realen Umgebungsbedingungen mit dem Demonstrationssystem durchgeführt wurden. Zur Gewährleistung von Sicherheit und der Zuverlässigkeit werden neben der satellitenbasierten Ortung weitere Sensordaten erfasst und mittels Kalmanfilterung fusioniert [Geistler 2006].

Grundgedanke für das System war die Konzeption eines homogenen und standardisierten Systems, welches nachhaltig und innovativ Kosten und Komplexität von Zugsicherungskonzepten und -systemen verringert. Um diesen Gedanken umzusetzen, muss die Fahrzeugortung auf den produktiven Elementen des Schienenverkehrs, den Fahrzeugen selbst, stattfinden. Aufgrund neuer Standards und Regularien, insbesondere auf die Sicherheitsaspekte bezogen, sind neue Vorgehensweisen bei Entwurf, Implementierung und Zulassung erforderlich, wodurch in Verbindung mit der Sensordatenfusion ein angestrebtes Sicherheitsniveau erreicht werden kann [Becker/Schnieder 2004].

Das Projektkonzept wurde wie folgt umgesetzt. Fahrzeugseitig wird mittels eines GNSS-Empfängers als primärer Sensor die satellitenbasierte Ortung (zukünftig durch GALILEO) eingesetzt. In Ergänzung ist unter dem Fahrzeug ein witterungsunabhängiger doppelter Wirbelstromsensor als wirbelstrominduzierendes System angeordnet, welches kontinuierlich metallische Gegenstände in der Umgebung des Schienenkopfes und der Schienenverschraubung detektiert bzw. Inhomogenitäten sensiert und als sekundäres Signal dem DemoORT-System zur Auswertung bereitstellt [Böhringer 2008], [Engelberg 2001]. Inhomogenitäten im metallischen Bereich der Schiene – etwa an Weichen – werden mit einer digitalen Karte als Referenzpunkte bzw. „virtuelle Balisen“ abgeglichen, wodurch die reale Position des Fahrzeugs bzgl. der Weichenlage erfasst werden kann [Becker et al. 2005], [Geistler 2006]. Mit Hilfe dieses „Map Matchings“, bei dem auf einer erweiterten digitalen Streckenkarte auch die Sensordaten aus der Satellitenortung ausgewertet werden, kann eine hochgenaue Positionsbestimmung des Fahrzeugs erreicht werden, welche die jeweiligen Einzelsensoren nicht erzielen. Ein weiterer Vorteil dieses Aufbaus ist die durchgängige Redundanz des Ortungssystems, welche dadurch tolerant gegenüber Ausfällen einzelner Sensoren werden. Durch die Auswertung der Daten der beiden kontinuierlich sendenden Wirbelstromsensoren ist über einen Korrelationsabgleich neben der kontinuierlichen Positionsbestimmung auch die Berechnung der Fahrzeuggeschwindigkeit und des zurückgelegten Weges umsetzbar und weiteren Systemen sicher und zuverlässig zur Verfügung gestellt werden. Bild 3.15 zeigt in a) den Wirbelstromsensor (S_1 und S_2) über dem Schienenkopf mit einer Gleisverschraubung und dem zugehörigen Sensorsignal, b) zeigt das Korrelationsprinzip.

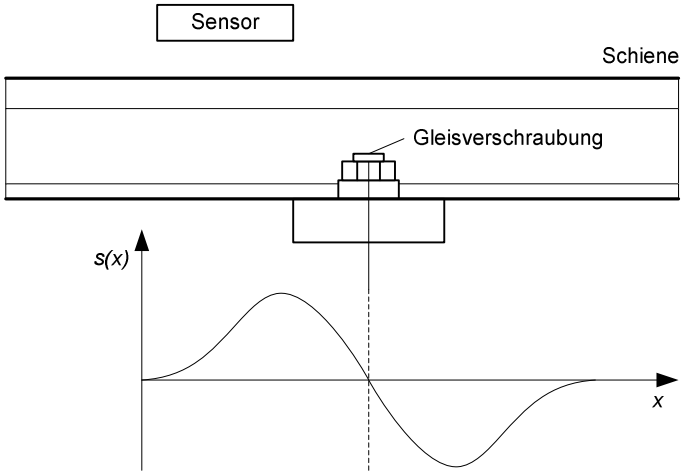

Bild 3.15 a): Sensorsignal über Gleisverschraubung nach [Geistler 2006]

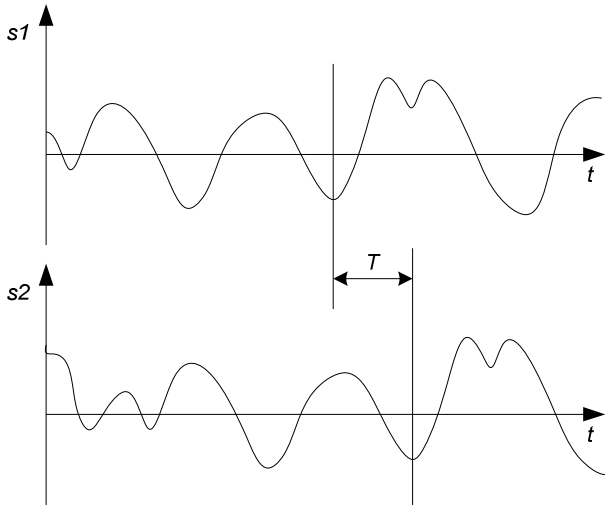

Bild 3.15 b): Korrelationssignal beider Sensoren

Der eigentliche Aufbau des DemoORT-Systems wird in Bild 3.16 (einschließlich der Sensordateninformationsflüsse) schematisch dargestellt.

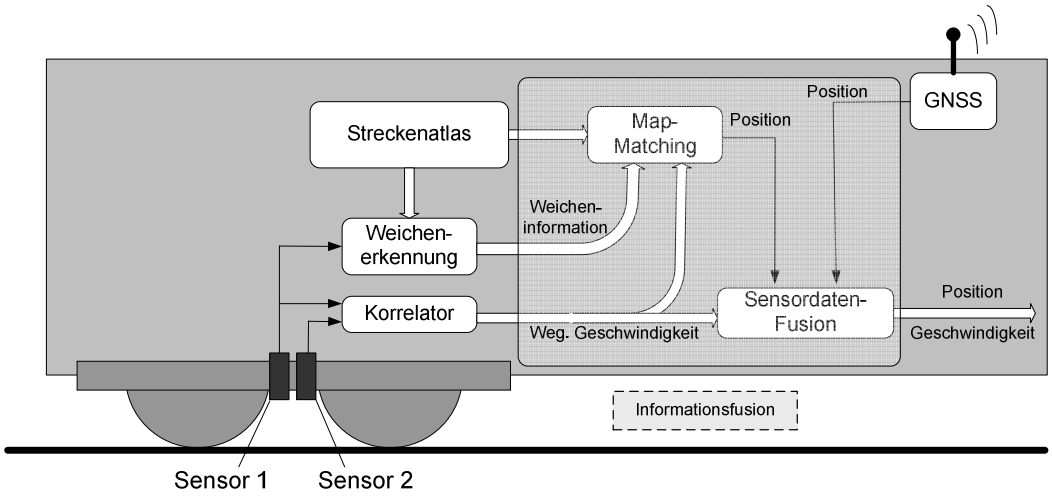

Bild 3.16: Datenfluss und Aufbau des DemoORT-Systems

Zur Verifikation der Teilsysteme und Valdierung des Gesamtsystems wurde am Institut für Verkehrssicherheit und Automatisierungstechnik (iVA) der Technischen Universität Braunschweig ein Referenzmesssystem konzipiert, welches für Langzeittests unter realen Bedingungen auf Testinfrastrukturen installiert wurde. Die Referenz-Plattform erfasst eigenständig mit zwei unterschiedlichen Sensoren die Positionsdaten des Fahrzeugs und analysiert diese mit einer separaten digitalen XML-basierten Streckenkarte [Poliak 2009]. Bei der Auswahl der Sensoren wurden die äußeren Anforderungen an das System sowie die systemspezifische Genauigkeit von +/- 0,5 m berücksichtigt. Als primärer Sensor wird ein Doppler-Radar eingesetzt, der aufgrund der relativ hohen Drift von etwa 0,2 % an Kalibrierungspunkten ausgeglichen werden muss. Für diese Kalibrierung wurden RFID-Transponder auf der Streckeninfrastruktur in Gleismitte fest installiert, mit einer maximalen Messabweichung von 2 cm vermessen und in der digitalen Streckenkarte berücksichtigt. Mit Hilfe der fahrzeugseitigen RFID-Antennen werden die Transponder bei der Fahrzeugüberfahrt identifiziert [Poliak 2009], [Hänsel et al. 2006].

Bild 3.17 zeigt den schematischen Aufbau des Braunschweiger Referenzmesssystems im und am Fahrzeug.

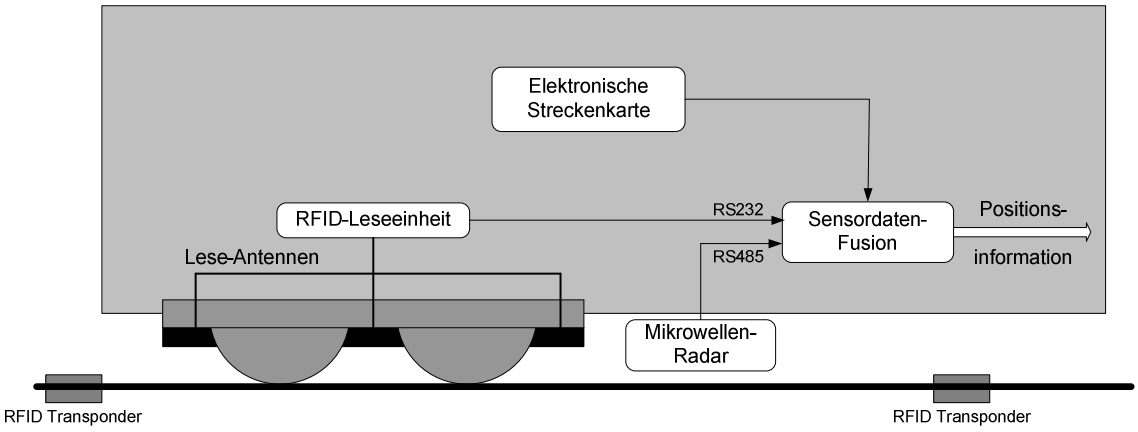

Bild 3.17: Referenzmesssystem zu DemoORT

Die für die zuverlässige Datenauswertung des Referenzmesssystems und des DemoORT-Systems benötigte Zeitsynchronisation wird mit Hilfe von GNSS-Daten umgesetzt. Im Testbetrieb werden die Positionsinformationen der beiden Systeme von einer Auswerteeinheit analysiert und geben Aufschluss über Verfügbarkeiten und Zuverlässigkeiten des DemoORT-Systems, wodurch im Nachgang Rückschlüsse auf die Sicherheit gezogen werden können.

Aufgrund der Planung des Einbezugs von GALILEO für den satellitenbasierten DemoORT-Systemteil ist die Verfügbarkeit des Signals in Verbindung mit der erforderlichen Qualität spezifiziert. Als Qualitätsparameter für das gesamte DemoORT-System wurden folgende Festlegungen getroffen:

- maximale Positionsabweichung: 0,5 m (bis Zuggeschwindigkeit 120 km/h)
- Drift bei Geschwindigkeitsmessungen: < 2 km/h (bis 30 km/h)
- Drift bei Geschwindigkeitsmessungen: Maximalwert 12 km/h (500 km/h)
- Lineare Drift zwischen 30 km/h und 500 km/h Zuggeschwindigkeit

Für die Weiterverarbeitung der sicheren Positionsdaten in übergeordneten Zugsicherungssystemen kann für die Anwendung im Betriebsverfahren des Zugleitbetriebs auf Nebenstrecken DemoORT als genaues Ortungssystem eines im Hintergrund agierenden Überwachungssystems bestehen, welches – unter Beibehaltung der bestehenden Betriebsverfahren – in Gefahrensituationen erforderliche Daten bereitstellt und automatisiert Zwangsbremsungen betroffener Züge bewirkt [Becker et al. 2005].

Als Zusammenfassung lassen sich für das DemoORT-Projekt folgende Thesen aufstellen, die die o.g. Innovationsgrundsätze bestärken und die bei der weiteren Betrachtung berücksichtigt werden müssen:

1. Sicherheit und Qualität der Ortung in Bezug auf Zuverlässigkeit, Genauigkeit und Verfügbarkeit müssen mindestens den Ansprüchen bisheriger, streckenseitiger Ortungsverfahren genügen.
2. Gewährleistung hochgenauer Positionsbestimmung des Fahrzeugs mit Erweiterbarkeit für die Zugschlussortung bei hoher Zuverlässigkeit und Lebensdauer.
3. Erhöhung von Streckenleistungsfähigkeiten und Verbesserung der Wirtschaftlichkeit des Gesamtsystems Bahn bei geringen Investitionskosten soll geleistet werden.

3.5.3 Gegenüberstellung ausgewählter Projekte

Zur abschließenden Betrachtung werden in der nachfolgenden Übersicht (Bild 3.18) die beiden ausgewählten Projekte vergleichend gegenübergestellt. Berücksichtigt werden dabei auch die jeweiligen Stärken und Schwächen in Bezug auf den Einsatz im Bahnbetrieb.

Zielsetzung	LOCOPROL	DemoORT
Anwendungsbereich	Nebenbahnen und ggf. für ETCS auf Hauptbahnen	Nebenbahnen und ggf. für ETCS auf Hauptbahnen
Redundanz	geringe Redundanz der Komponenten	hohe Systemredundanz durch parallel arbeitende Sensoren
Integrität	durch Verwendung der Signale unterschiedlicher Satelliten	durch Sensordatenfusion
Kostenreduktion	keine streckenseitigen Einrichtungen, Verbesserung der Wirtschaftlichkeit, Reduzierung der Kosten für die Kommunikation	keine streckenseitigen Einrichtungen, Verbesserung der Wirtschaftlichkeit
Betriebsverfahren	mit absolutem Streckenblock	ohne Streckenblock
Stärken	- Kostenreduzierung im Gesamtsystem - Steigerung der Sicherheit - geringe Systemredundanz führt zu geringeren Kosten - Kostensenkung durch Reduzierung der Kommunikation - Interoperabilität mit ERTMS/ ETCS	- Kostenreduzierung im Gesamtsystem - Steigerung der Sicherheit - hohe Genauigkeit der Ortung - (Interoperabilität mit ERTMS/ ETCS)
Schwächen	- Genauigkeit der Ortung nur innerhalb eines Konfidenzintervalls	- hohe Systemredundanz führt zu höheren Kosten

Bild 3.18: LOCOPROL und DemoORT im Projektvergleich

Nach Abwägung von Stärken und Schwächen der gewählten Projekte wird erkennbar, dass die im Projekt DemoORT gewählte Kombination aus GNSS-Empfänger, Wirbelstromsensorik und digitaler Karte sämtliche Anforderungsbereiche für ein leistungsfähiges Sicherungssystem abdeckt. Auch die Beachtung der zusammenfassenden Thesen aus Abschnitt 3.5.2 lassen sich mit DemoOrt vermutlich umsetzen. Für die exemplarische Sicherheitsuntersuchung gilt DemoOrt als Bezugssystem.

3.6 Innovationspotenziale der fahrzeugautarken Ortung

Mit Hilfe der fahrzeugautarken Ortung sollen die in Bild 1.2 herausgestellten drei Größen der Sicherheit, Streckenleistungsfähigkeit und Betriebskosten sinnvoll in Einklang für einen zukunftsweisenden Schienenverkehr gebracht werden.

Aufgrund der größtenteils menschlichen Sicherungsfunktionen, realisiert durch das Betriebspersonal, hat der Zugleitbetrieb (ZLB) enormes Potenzial für Innovationen. Durch den ergänzenden Einsatz von einfachen Sicherungssystemen lässt sich die Leistungsfähigkeit von Nebenbahnen erhöhen. Insbesondere auf dem Gebiet der erweiterten Sicherungstechnik im „Low-Cost“-Bereich sind Potenziale der fahrzeugautarken Ortung erkennbar, da sie sich direkt gegen die Erhöhung der Streckenleistungsfähigkeit bewerten lassen. Die Zugintegritätsprüfung kann unter Umständen sogar vernachlässigt bzw. vereinfacht werden, sofern der für eine Strecke vorgesehene Fahrzeugpark (z.B. Triebwagenbetrieb) dies zulässt.

Aber auch außerhalb des ZLB lässt sich eine Vielzahl an betrieblichen Innovationspotenzialen erkennen. Die Möglichkeiten für den Einsatz sicherheitsrelevanter Ortung im Schienenverkehr sind weitreichend, da die Nutzenpotenziale in allen Bereichen der Transportprozesse wieder zu finden sind. Durch eine Verlagerung der Ortung auf die Fahrzeuge sind innovative Ansätze vorrangig im Bereich der Verfolgbarkeit der Fahrzeugstandorte zu nennen [Becker/Schnieder 2004], [Schnieder/Barbu 2009].

Die derzeit bereits im Einsatz befindliche fahrzeugautarke Ortung im Schienenverkehr dient vorrangig der Information von Fahrgästen oder Güterverkehrskunden mit nicht sicherheitsrelevanten Daten, wie z.B. Bahnhofsansagen [Becker/Schnieder 2004] oder Zustandsinformationen des Transportgutes im Güterverkehr [Hartwig et al. 2005], [Hänsel et al. 2007], [Schnieder/Barbu 2009]. Übergeordnete Systeme stellen die Ortungsinformationen dem Nutzer entsprechend zur Verfügung. Hervorzuhebende Anwendungen sind die Erfassung und Protokollierung der ortsabhängigen Fahrdaten auf dem Triebfahrzeug, welche u.a. nach Unregelmäßigkeiten im Bahnbetrieb für Aufklärung sorgen, sowie ortsgenaue Spurkranzschmierungen und Fahrzeugneigesysteme. Durch die ortsgenaue Auftragung von Schmierstoffen im Kurvenbereich auf die Spurkränze der Fahrzeuge kann der Schmierstoffverbrauch minimiert und die Umweltbelastung dementsprechend reduziert werden. Eine optimierte radiengenaue Ansteuerung der Neigetechnik im Fahrzeug würde vorrangig den Reisekomfort für die Fahrgäste im Fahrzeug weiter verbessern. Mittels der genauen Ortung könnten auch Sandungsanlagen der Triebfahrzeuge im Bereich von Weichen funktionsunterdrückt werden, wodurch Reinigungen der Weichenanlagen entfielen.

Auch für das komplexe Feld der Disposition stellt die genaue Fahrzeugortung die entscheidende Basis dar. Je exakter eine zuverlässige Aussage über die aktuelle Position eines Zuges gegeben werden kann, desto verlässlicher und beschleunigter können betriebliche Konflikte gelöst werden, wodurch letztlich die Leistungsfähigkeit der bisherigen Strecken ohne infrastrukturellen Mehraufwand gesteigert werden könnte [Wegele 2005]. Zur weiteren Energieeinsparung [Sanftleben et al. 2001] und Optimierung der Streckenkapazitäten werden zukünftig Systeme zur Fahrtoptimierung auf den Triebfahrzeugen eingesetzt (vgl. Projekt Free-Float der DB AG) [Oetting 2008]. Hinter der Bezeichnung „Driving Style Manager“ verbirgt sich ein System, welches Ortungsinformationen und Daten aus der streckenseitigen Disposition in Geschwindigkeits-Soll-Vorgaben für den Eisenbahnfahrzeugführer umsetzt. Auch im Rahmen von turnusmäßigen Infrastrukturprüfungsfahrten können bei Unregelmäßigkeiten auf der Streckeninfrastruktur die genauen Ortungsinformationen mittels fahrzeugautarker Ortung an das Infrastrukturunternehmen übertragen werden [Schnieder/Barbu 2009].

Für innovative Verwendungen im Schienenverkehr lässt sich eine Vielzahl weiterer Potenziale im Bereich der sicherheitsrelevanten Anwendungen herausstellen. Im Bereich der Sicherung von Gleisbaustellen während des Betriebes würden innovative Rottenwarnsysteme, die auf Ortungsinformationen über sich nähernde Fahrzeuge zurückgreifen könnten, ein quantifizierbares Sicherheitspotenzial für die Mitarbeiter realisieren, was beispielsweise zu Einsparungen auf Seiten der Versicherungswirtschaft führte. Mit der Weiterentwicklung von Kollisionsvermeidungs-

systemen auf Basis der sicherheitsrelevanten Ortung (System RCAS (Railway Collision Avoidance System) – Deutsches Zentrum für Luft- und Raumfahrt) wären zusätzliche Kosteneinsparungen auf der Versicherungsseite zu erzielen [DLR 2009]. Fahrzeugsseitige Integritätsprüfungen beinhalten selbst auch ein Innovationspotenzial, da sie sich nachhaltig auf die Leistungsfähigkeit der Streckeninfrastrukturen auswirken. Ist-Zeit-gerechte Fahrplanung wie auch ein Online-Trassenmanagement wären durch eine sichere und verlässliche Ortungsinformation möglich. Ansätze wurden dazu bereits im Projekt „FreeFloat“ der Deutschen Bahn AG entwickelt [Oetting 2008]. Mit Hilfe der fahrzeugseitigen Ortungsinformation in Verbindung mit der Zuggeschwindigkeit können Bahnübergänge zeitabhängig und nicht – wie derzeit üblich – wegabhängig eingeschaltet werden, wodurch die Schließzeiten von Bahnübergängen vereinheitlicht werden könnten, was nachhaltig die Sicherheit an Bahnübergängen erhöhte. Dieser Ansatz wurde erstmals im Projekt Funk-Fahr-Betrieb (FFB) der Siemens AG im Jahr 2000 in einem Pilotversuch umgesetzt [Pachl 2004]. Im Netz der Deutschen Bahn AG existieren derzeit noch ca. 22.000 Bahnübergänge [Selcat 2007]. Könnten die Wartezeiten für den Straßenverkehr verringert werden, würde sich nicht nur die Sicherheit erhöhen – sondern auch volkswirtschaftlich gesehen – ein finanzieller Gewinn entstehen, da sich die Verfügbarkeit vergrößerte.

Ein abschließendes und bedeutendes Potenzial ist die Informationsbereitstellung für Zugsicherungssysteme (Leit- und Sicherungstechnik). Mittels genauer und verlässlicher Ortungs-information, welche auch die Zugintegrität und die Gleisselektivität einschließt, können innovative Sicherungssysteme, wie u.a. ETCS für den Level 3, weiterentwickelt werden, womit sich die Leistungsfähigkeit der Strecken erheblich steigern ließe und bei gleichbleibender Infrastruktur die Mindestzugfolgezeiten [Schnieder 2007] extrem reduziert werden könnten. Auch der Aspekt der Interoperabilität in Europa wäre durch ein innovatives Ortungssystem in Verbindung mit ETCS Level 3 berücksichtigt [Meyer zu Hörste 2004].

Bild 3.19 stellt eine Übersicht über die vorgestellten Anwendungspotenziale dar. Die verschiedenen Nutzer der Systeme, unterschieden nach Eisenbahnverkehrsunternehmen (EVU), Infrastruktur-unternehmen (EIU) sowie dem Endkunden, sind aufgeführt und mit einer Bewertung der Potenzialnutzung versehen.

			Nutzenverteilung		
Übergeordnetes Anwendungspotenzial	**Sicherheits-relevantes System**	**Übergeord-netes System**	**Eisenbahn-Infrastruktur-Unternehmen (EIU)**	**Eisenbahn-Verkehrs-Unternehmen (EVU)**	**Güterverkehrs-kunde / Reisender**
Fahrgastinformation		x	---	++	+++
Transportgutverfolgung		x	---	++	+++
Ortsgenaue Fahrdatenprotokollierung		x	+++	+++	---
Spurkranzschmierung		x	++	+++	---
Neigezugtechnik	(x)	x	++	+	+++
Sandungseinrichtung		x	+++	++	---
Dispositionsunterstützung		x	+++	+++	+++
Ad-hoc-Trassenmanagement (Free-Float)		x	+++	+++	+
Fahrtoptimierung (Driving-Style-Manager)		x	++	+++	+
Infrastrukturprüfung	x	(x)	+++	---	---
Baustellensicherung	x		+++	---	---
Bahnübergangssicherung	x		+	+	+++
Zugsicherungssysteme	x		+++	+++	++
ETCS Level 3	x		+++	+++	++

+ Nutzungspotenzial erkennbar, ++ nachhaltiges Nutzungspotenzial, +++ vorrangiges Nutzungspotenzial, --- kein Potenzial erkennbar

Bild 3.19: Anwendungspotenziale und Nutzen innovativer fahrzeugautarker Ortung [Becker/Schnieder 2004]

Die Nutzungspotenziale aus Bild 3.19 beinhalten noch nicht aufzuwendende Kosten für eine Realisierung, da diese momentan nur schwer quantifizierbar sind. Tatsache ist aber, dass sich Kosten durch die Verlagerung von Funktionen von der Infrastruktur auf die Fahrzeuge ebenfalls zwischen Infrastrukturunternehmen (EIU) und Verkehrsunternehmen (EVU) verlagern werden.

Zur Realisierung der Potenziale – insbesondere für sicherheitsrelevanten Anwendungen – sind für das fahrzeugautarke Ortungssystem primär hohe Ortungsgenauigkeiten, verbunden mit einer hohen Systemverfügbarkeit sowie einer kontinuierlichen Zugintegritätsprüfung, erforderlich und nachzuweisen. Bild 3.20 aus [Klinge 1997] verdeutlicht die Potenziale und Notwendigkeit für eine nachhaltige Anwendung innovativer Zugsicherungssysteme auf der Grundlage von ETCS Level 3. Deutlich wird der Unterschied zwischen den Streckenleistungsfähigkeiten bei der Ortung mit Blocksicherungsverfahren und dem innovativen Ortungsansatz mit einem neuen Sicherungssystem. Unter Berücksichtigung dieses Ansatzes ist auch der innovative Zugverkehr mittels virtuell gekuppelten Zügen, wie im Projekt „Bahn 2050“ vorgestellt, umsetzbar [König 2050].

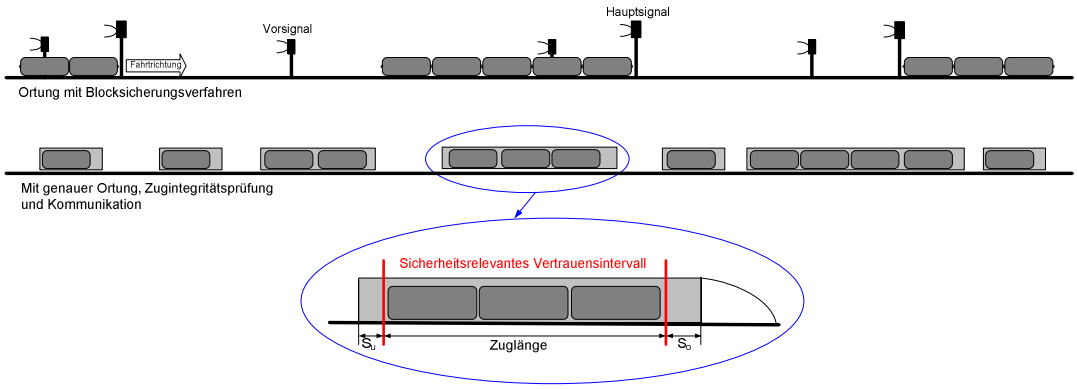

Bild 3.20: Streckenleistungsfähigkeit und Mindestzugfolgeabstand im Vergleich [Klinge 1997]

Der in Bild 3.20 dargestellte Ansatz steht stellvertretend auch für Eisenbahnstrecken mit ZLB. Allerdings muss dabei der eingleisige Betrieb berücksichtigt werden.

Zusammenfassend sind durch Umsetzung der Potenziale folgende Vorteile zu nennen:

- Geringere Zugfolgeabstände (Mindestzugfolgezeiten) bei höheren Fahrgeschwindigkeiten
- Höhere Streckenkapazitäten mit größerer Streckenauslastung
- Sicherheitsgewinn
- Verringerter Verschleiß an Fahrzeugen und Strecken
- Geringere Investitions- und Instandhaltungskosten an Fahrzeugen und Infrastruktur
- Erhöhung der Dispositionsflexibilität und Qualität des Reisens
- Sinkende Umweltbelastung und Umfeldstörungen
- Geringere Kosten für Unternehmen
- Umfassendere und zeitgerechtere Informationsmöglichkeit für alle Beteiligten

Ersichtlich wird, dass mittels der satellitengestützten, fahrzeugautarken Ortung allen beteiligten Gruppen Vorteile für einen innovativen Schienenverkehr geboten werden können. Die Attraktivität des Schienenverkehrs kann dadurch gegenüber anderen Verkehrsarten innovativ gesteigert werden. Sicherheit, Genauigkeit und Verfügbarkeit des Ortungssystems sind dabei die Grundlage.

4 METHODISCHE GRUNDLAGEN ZUR VERLÄSSLICHKEITSBESTIMMUNG

Zur Realisierung fahrzeugautarker Ortungssysteme mit Sicherheitsrelevanz, welche sich in das komplexe Umfeld der Automatisierungs- und Schienenverkehrstechnik eingliedern sollen – beim letzteren insbesondere in den Bereich der Sicherungstechnik – ist die Betrachtung der Verlässlichkeit unumgänglich. Verlässlichkeit in Automatisierungssystemen im Sinne der Eigenschaften Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS: Reliability, Availability, Maintainability, Safety) erweist sich bei komplexen Automatisierungssystemen zunehmend als entscheidender Faktor von Wirtschaftlichkeit, Betriebs- und Produktqualität [EKA 2003].

Im Schienenverkehr hat sich spätestens mit der Einführung der CENELEC-Normen (vgl. Abschnitt 2.4) die Betrachtung der Verlässlichkeit unter der Kurzbezeichnung „RAMS“ mit zunehmender Bedeutung für Zulassungsverfahren durchgesetzt. Die Norm DIN EN 50126 [EN 50126] für Eisenbahnanwendungen verlangt zur Spezifikation und zum Nachweis hoher Qualitäts- und Sicherheitsanforderungen ein gemeinsames Verständnis und eine Vorgehensweise für Hersteller und Betreiber von Bahnsystemen ein RAMS-Management.

4.1 Definitionsabgrenzung

Im Folgenden wird eine Vielzahl von Begriffen aus dem Umfeld der Verlässlichkeit verwendet. Zur Definition der Begriffe findet sich an dieser Stelle eine taxonomische Einordnung (Bild 4.1), die auf dem methodischen Ansatz von [Schnieder 2008] beruht.

Die Klassifizierung der Begriffe erfolgt in Zustands- und Eigenschaftsabgrenzungen, die in ihrem Begriffsinhalt statische Zustände bzw. Eigenschaften beschreiben sowie Prozess- bzw. Verfahrensbegriffe, die mit ihrem Begriffsinhalt ihrerseits dynamische Vorgehen, Prozesse und Methoden hervorheben.

	Begriff	Definition	Quelle
Zustands- / Eigenschaftsbegriffe	Gefährdung	Eine physikalische Situation, die potenziell einen Schaden für den Menschen beinhaltet bzw. eine Bedingung, die zu einem Unfall führen kann.	DIN EN 50129
	RAMS	Engl. für Reliability, Availability, Maintainability und Safety	DIN EN 50126
	Risiko	Die Wahrscheinlichkeit des Auftretens einer Gefährdung, die einen Schaden verursacht, sowie der Schweregrad des Schadens.	DIN EN 50126
	Safety Integrity Level (SIL)	Eine festgelegte Anzahl diskreter Stufen für die Spezifizierung der ausreichenden Sicherheit von Sicherheitsfunktionen, die sicherheitsrelevanten Systemen zugeordnet sind. Der SIL mit der höchsten Ordnungsziffer hat den höchsten Level der ausreichenden Sicherheit.	DIN EN 50126
	Schaden	Ein Schaden ist eine Minderung oder der Verlust an materiellen oder immateriellen Gütern z.B. durch Unfall.	
	Sicherheit (safety)	Sicherheit ist das Nichtvorhandensein eines unzulässigen Schadensrisikos.	DIN EN 50126
	Sicherheitsrelevantes System	Das System trägt Sicherheitsverantwortung.	DIN EN 50129
	System (-eigenschaften)	Menge von Teilsystemen, die entsprechend einem Entwurf zusammenwirken.	DIN EN 50129
	tolerierbares Risiko	Der maximale für ein Bahnunternehmen tolerierbare Grad an Risiko durch ein System.	DIN EN 50129
	Verfügbarkeit (availability)	Die Fähigkeit eines Systems, in einem Zustand zu sein, in dem es unter vorgegebenen Bedingungen zu einem vorgegebenen Zeitpunkt oder während einer vorgegebenen Zeitspanne eine geforderte Funktion unter der Voraussetzung erfüllen kann, dass die geforderten äußeren Hilfsmittel bereitstehen.	DIN EN 50126
	Zuverlässigkeit (reliability)	Die Wahrscheinlichkeit dafür, dass eine Einheit ihre geforderte Funktion unter gegebenen Bedingungen für eine gegebene Zeitspanne (t1, t2) erfüllen kann.	DIN EN 50126

	Begriff	Definition	Quelle
Prozess- / Verfahrensbegriffe	Gefährdungsanalyse	Prozess der Identifikation von Gefährdungen und der Analyse ihrer Ursachen sowie der Ableitung von Anforderungen, um die Wahrscheinlichkeit und die Folgen von Gefährdungen auf ein akzeptables Maß zu begrenzen.	DIN EN 50129
	Risikoanalyse	Analytische Abschätzung von Risiken als Bestandteil der Sicherheitsanalyse.	
	Sicherheitsanalyse	Methodengestützte Analyse der Sicherheit eines Systems.	
	Sicherheitsbetrachtung	Betrachtung der Systemsicherheit ohne methodisches Vorgehen.	
	Sicherheitsbewertung	Abschließende Bewertung der Sicherheit als Ergebnis einer Sicherheitsuntersuchung.	
	Sicherheitsnachweis	Dokumentierter Nachweis, dass das System die spezifizierten Sicherheitsanforderungen erfüllt.	DIN EN 50129
	Sicherheitsnachweis (-führung)	Dokumentierter Nachweis, dass das System die spezifizierten Sicherheitsanforderungen erfüllt.	DIN EN 50129
	Sicherheitsprozess	Reihe von Verfahren, deren Abfolge sicherstellt, dass die Sicherheitsanforderungen eines Systems identifiziert und erfüllt werden.	DIN EN 50129
	Sicherheitsuntersuchung	Methodische Kombination aus Sicherheitsanalyse und Sicherheitsnachweis.	
	Validierung	Bestätigung durch Überprüfung und objektiven Nachweis, dass die besonderen Anforderungen für einen spezifischen, bestimmungsgemäßen Gebrauch erfüllt wurden.	DIN EN 50126
	Verifikation	Bestätigung durch Überprüfung und objektiven Nachweis, dass die festgelegten Anforderungen erfüllt wurden.	DIN EN 50126

Bild 4.1: Begriffsdefinitionen im Umfeld der Verkehrssicherheit

Weiter vertiefende Begriffsdefinitionen sind in den Normen sowie u.a. in [Braband 2005], [Slovak 2007] und [Schnieder 2009] zu finden.

Die Prozess-/Verfahrensbegriffe stehen dabei in einer engen Relation zu den Zustands-/Eigenschaftsbegriffen. In der Gesamtheit ergeben die in der Relation stehenden Begriffe ein so genanntes Begriffssystem, welches zum Verständnis und zur Eindeutigkeit des erforderlichen Wissens domänenunspezifisch beiträgt. Ein anschauliches Beispiel für eine Begriffsmenge wird in Bild 4.2 vorgestellt.

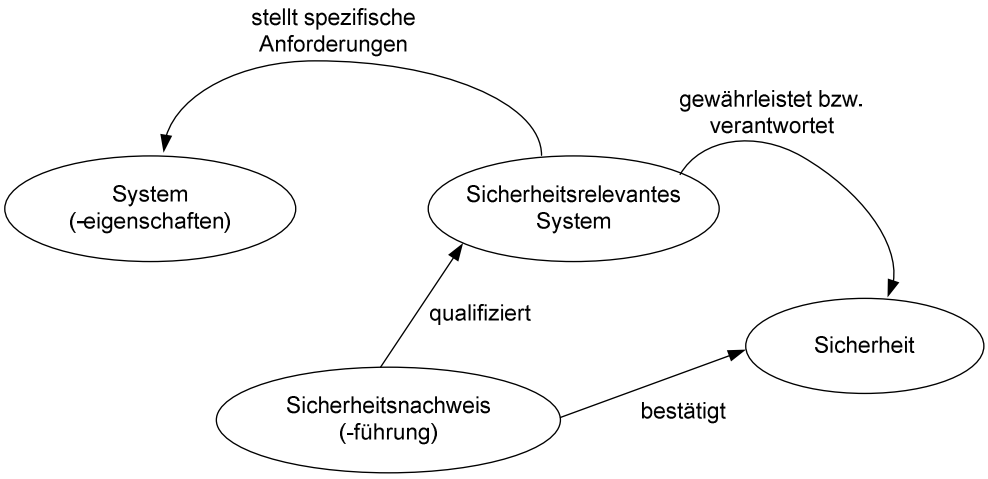

Bild 4.2: Exemplarisches Begriffssystembeispiel

Eine detaillierte Erläuterung zum Themenfeld der Begriffssystemmodellierung im Zusammenhang mit der Verkehrssicherheit in einem systemischen Kontext liefern u.a. [Drewes 2009] und [Schnieder L 2009]. Im Rahmen der vorliegenden Arbeit werden diese Begriffe hingegen nur zur Veranschaulichung und zur Klärung der Begriffsinhalte verwendet. Auf die unterschiedlichen Ausprägungen der Begriffsrelationen sowie die Konstruktion von Begriffssystemen wird an dieser Stelle verzichtet.

4.2 Grundlagen der Sicherheitsuntersuchung

Zur Umsetzung des gemeinsamen Verständnisses zwischen dem Systemhersteller und -betreiber wird der Systemlebenszyklus als V-Modell (Bild 4.3) als normative Grundlage angesehen. Während der Bahnbetreiber für sein gewünschtes System ein Lastenheft mit der Konzeption, der Definition des Systems und der Anwendung, der Risikoanalyse sowie den Systemanforderungen zusammenstellt und sich damit befasst, wie das System später abgenommen werden wird, der Betrieb und die Instandhaltung zu erfolgen und ggf. eine Entsorgung auszusehen hat, werden durch den Hersteller in Form eines Pflichtenheftes die Anforderungen bestätigt, das Systems entwickelt, installiert und validiert sowie sicherheitsuntersuchend begleitet. Die Abgrenzung jeder Phase erfolgt durch phasenbezogene Verifikationsschritte [Drewes/May 2007].

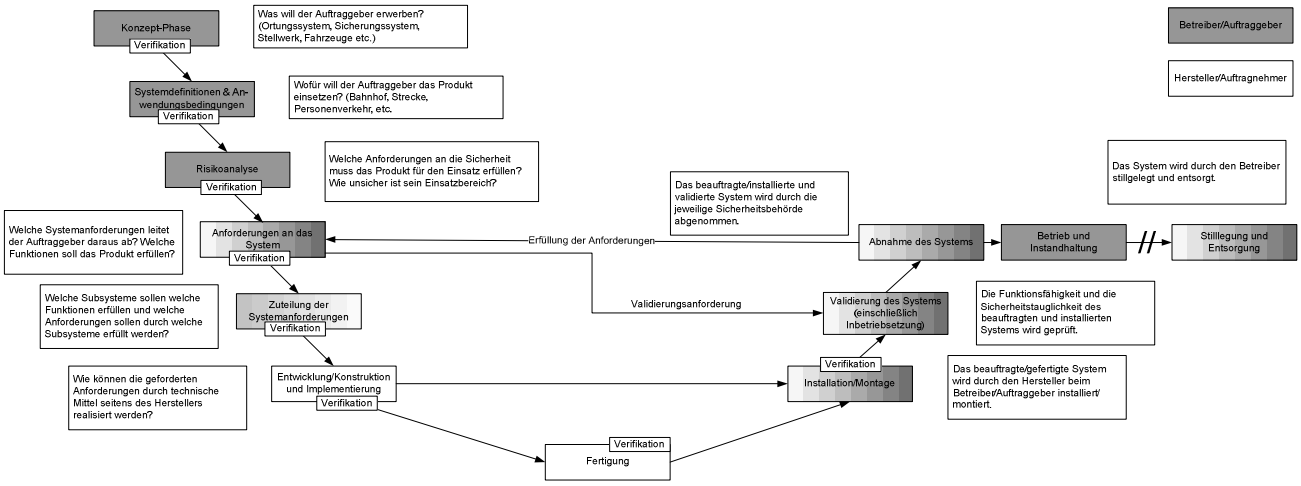

Bild 4.3: Systemlebenszyklus als V-Modell, angelehnt an DIN EN 50126

Der gesamte Systemlebenszyklus sollte sowohl durch den Hersteller als auch durch den Systembetreiber nach den RAMS-Kriterien durchdrungen werden, da die Qualität des Systems und somit die Qualität der späteren Betriebsleistung eines übergeordneten Systems entscheidend von den RAMS-Eigenschaften abhängt. Dies spiegelt sich bereits im Grundsatz des Eisenbahnverkehrs durch die drei Zielparameter Sicherheit, Pünktlichkeit (Verfügbarkeit) und Wirtschaftlichkeit wider (vgl. Abschnitt 1.2), wobei die ersten beiden Aspekte bereits die relevanten Bestandteile der Verlässlichkeit darstellen. Sicherheit und Verfügbarkeit stehen übergeordnet in enger Abhängigkeit und werden von der Zuverlässigkeit der Systemkomponenten sowie der Realisierung der Systeminstandhaltung beeinflusst [Drewes 2009], [Schnieder 2009].

Für die Entwicklung eines verlässlichen und sicherheitsrelevanten Systems sind nach CENELEC anfänglich die Phasen zwei (Systemdefinition) bis fünf (Zuteilung der Systemanforderungen) des V-Modells (Bild 4.3) näher zu untersuchen. Diese umfassen den Bereich der Sicherheitsanalyse, in dem die sicherheitsrelevanten und projektbezogenen Anforderungen zwischen dem späteren Betreiber und dem Hersteller des Systems unter Berücksichtigung legislativer Vorgaben ausgetauscht werden. In der traditionellen Entwicklung der Eisenbahnen hatte sich ein qualitatives Verständnis für die Sicherheit etabliert. Mit „sicher“ oder „nicht sicher“ wurden Systeme bewertet und entsprechend wurde potenziellen Gefährdungen begegnet [Müller 2006]. Moderne Ansätze der Sicherheitsanalysen basieren auf der funktionalen Untersuchung technischer Systeme mit der methodischen Ermittlung des betrieblichen Risikos als relative Wahrscheinlichkeitsgröße. Ausgehend von der projektbezogenen Gefährdungsidentifikation, ggf. unter Zuhilfenahme einer Gefährdungsliste, sind potenziell gefährliche Situationen zu analysieren und zu quantifizieren. In Form einer Risikoanalyse sind dabei durch den Bahnbetreiber die für sein Unternehmen vertretbaren funktionalen Sicherheitsziele für das zu betrachtende System im zugehörigen Anwendungsfall zu belegen. Bezeichnet als tolerierbare Gefährdungsraten (THR = Tolerable Hazard Rate) werden diese quantitativ den jeweiligen Funktionen zugeordneten Werte dem Hersteller als mindestens zu erreichende Zielgrößen übergeben [Drewes/May 2007], [Slovak 2007].

Einfluss bei der Ermittlung der tolerierbaren Gefährdungsraten haben bei den Betreibern u.a. die Sicherheitsphilosophien des jeweiligen Unternehmens, die jeweils stark durch Unfallereignisse des vorangegangen Zeitraums geprägt werden; ein anderer, gegenläufiger Faktor ist der Aufwand, der durch das systembetreibende Unternehmen zu leisten wäre. In diesem Fall ist es möglich – und in der Praxis weit verbreitet – auf eine detaillierte Risikoanalyse gänzlich zu verzichten und das höchste in der CENELEC-Norm geforderte Sicherheitsmaß in Form des Sicherheitsintegritätslevels (SIL) für das Gesamtsystem zu fordern. Dadurch wird es vermutlich teurer und bei der funktionalen Sicherheit überdimensioniert umgesetzt, was nach dem CENELEC-Ansatz verhindert werden sollte.

Auf Herstellerseite werden die tolerierbaren Gefährdungsraten mittels Anforderungsanalysen den sicherheitsrelevanten Funktionen zugeteilt und mit einer System-Gefährdungsanalyse belegt. Die Ergebnisse werden in der technischen Systemspezifikation inklusive der Spezifikation der Systemsicherheitsanforderungen im Pflichtenheft verbrieft. Zur Verdeutlichung zeigt Bild 4.4 den Prozess der Sicherheitsanalyse zwischen Betreiber und Hersteller.

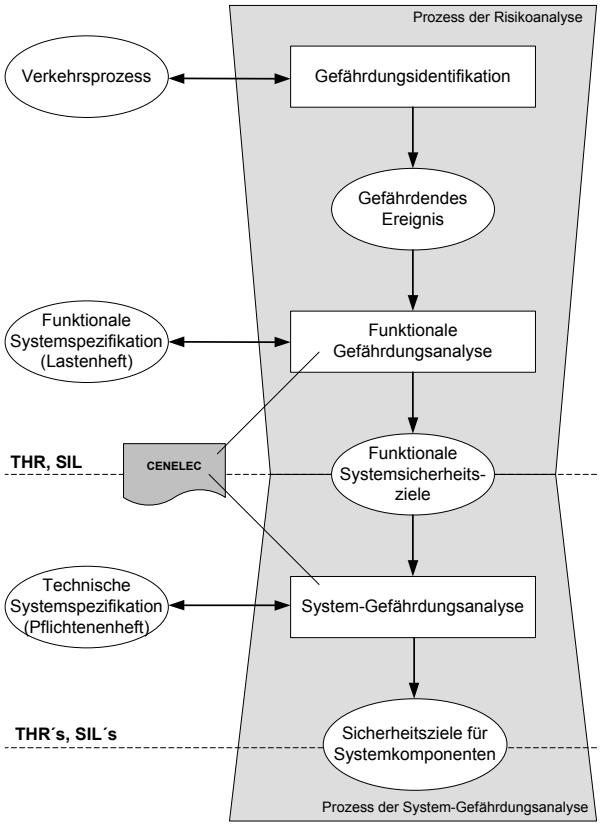

Bild 4.4: Prozessstruktur der Sicherheitsanalyse bei Bahnsystemen nach [Slovak 2007]

Ergänzend ist als begleitende Dokumentation während des gesamten Lebenszyklus ein Sicherheitsnachweis nach [EN 50129] durch den Hersteller zu erstellen, welcher für die Inbetriebnahme bzw. Systemzulassung die Umsetzung der Sicherheitsanforderungen nachweist. Vor der Einführung der CENELEC-Normen wurden bei der Sicherheitsnachweisführung aufgestellte, relativ einfache Sicherheitsanforderungsregeln qualitativ dahingehend bewertet, ob ein

anzunehmender und zu beherrschender Fehler einen sicheren Zustand herbeiführen würde. Mit der Einführung von softwaregestützten Systemen im Schienenverkehr wurde mit der [Mü 8004] durch das damalige Bundesbahnzentralamt ein komplexes Regelwerk zur Beherrschung der Systemsicherheit geschaffen. Ein innovativer Ansatz war damals die Aufnahme einer differenzierten Betrachtungsweise nach dem Maß der erforderlichen Sicherheit [Braband 2005].

Unabhängig vom zu untersuchenden System sind heute folgende Aspekte bei jeder Sicherheitsuntersuchung zu berücksichtigen:

- Analyse des Gesamtsystems
- geeignete Funktionsabgrenzung
- Analyse und Extraktion der entscheidenden Systemkomponenten
- Festlegung der Systemtiefe für qualitative und quantitative Aussagen
- Berücksichtigung des relevanten normativen Umfeldes
- Festlegung des Grenzrisikos („Wie sicher ist sicher genug?“)

Auch die jeweilige Sicherheitsphilosophie des Unternehmens sowie eine gelebte Sicherheitskultur sind entscheidende Vorgaben, die bei der Untersuchung Einfluss nehmen sollten [Müller 2006].

4.2.1 Beschreibungsmittel und Methoden

Im Rahmen von Sicherheitsuntersuchungen sind u.a. Gefährdungs- und Risikoanalysen durchzuführen. Da die Schriftsprache als alleiniges Beschreibungsmittel zu Mehrdeutungen führen kann, ist dabei die Anwendung geeigneter formaler Beschreibungsmittel [Schnieder 2007] und Methoden zielführend, die teilweise auch normativ vorgeschrieben sein können [EN 50128].

Die [IEC 60300-3-1] vergleicht die gebräuchlichsten Analysemethoden und Beschreibungsmittel bezüglich ihrer Eignung für die Anwendung bei Sicherheitsuntersuchungen. Bild 4.5 gibt einen Überblick über die Eignung der Methoden und Beschreibungsmittel.

Analysemethode:	Gefährdungsanalyse	Risikoanalyse
ETA (Ereignisbaum-Analyse)	möglich	geeignet
FME(C)A (Failure Mode and Effects (and Criticality) Analysis)	geeignet für serielle Systeme ohne Redundanz	geeignet für serielle Systeme ohne Redundanz
FTA (Störungsbaum-Analyse)	geeignet	möglich
HAZOP (Hazard and Operability Study)	nicht geeignet	nicht geeignet
Beschreibungsmittel:		
Markov-Modelle	geeignet	geeignet
Petrinetze Kanal-Instanzen Netze	geeignet	geeignet
RBD (Zuverlässigkeits-Block- Schaltbilder)	geeignet für nicht reparierbare Systeme	nicht geeignet

Bild 4.5: Analysemethoden zur Sicherheitsuntersuchung nach [IEC 60300-3-1]

Methoden wie Ereignisbaum-, Störungsbaumanalyse oder auch FME(C)A haben sich in der Praxis vorrangig in Kombinationsanwendungen bewährt.

Petrinetze oder auch Markov-Modelle als Beschreibungsmittel sind für eine methodische Anwendung alleinstehend geeignet; aufgrund ihrer komplex wirkenden Struktur werden sie in der Praxis aber meist nur untergeordnet berücksichtigt. Bild 4.6 zeigt diesen Sachverhalt anhand der vorherrschenden Eigenschaften der ausgewählten Analysemethoden und Beschreibungsmittel auf.

Analysemethode / Beschreibungsmittel	Eignung für komplexe Systeme	Qualitative Analyse	Quantitative Analyse	Eignung von Ausfallkombinationen	Betrachtung von Reihenfolgeabhängigkeiten möglich	Erforderliches Fachwissen für formale Technik	Akzeptanz und Gebräuchlichkeit	Toolunterstützung erforderlich	Standardisierung
Petrinetze, (z.B. Kanal-Instanzen Netze)	ja	ja	ja	ja	ja	hoch	mittel	ja	u.a. IEC 62551
ETA (Ereignisbaum-Analyse)	bedingt	ja	ja	nein	ja	hoch	mittel	bedingt	DIN 25419 IEC 62502
FTA (Störungsbaum-Analyse)	ja	ja	ja	ja	nein	mittel	hoch	bedingt	IEC 61025, DIN 25424
Markov-Modelle	bedingt	ja	ja	ja	ja	hoch	mittel	ja	IEC 61165
FMEA / FMECA (Failure Mode and Effects Analysis)	nein	ja	nein / ja	nein	nein	gering	hoch	nein	IEC 60812

Bild 4.6: Eigenschaften ausgewählter Analysemethoden und Beschreibungsmittel nach [May 2002], vgl. auch [Braband 2005], [Slovak 2007]

In der Automatisierungstechnik hat sich das so genannte „BMW-Prinzip“ etabliert, wodurch der Zusammenhang zwischen einem Beschreibungsmittel (B), einer zugehörigen Methode (M) und dem dazu erforderlichen Werkzeug (W) dargestellt wird. Die nicht zufällige Verwandtschaft der Namensgebung zu einer bekannten Automobilmarke unterstreicht Fortschritt und Modernität formaler Techniken [Schnieder 1999]. Mit dem Begriff „formale Technik“ werden (formale) Beschreibungsmittel und Methoden zusammengefasst. In den Bildern 4.5 und 4.6 wurden formale und semiformale Beschreibungsmittel und Methoden vorgestellt. Tiefer gehender Ergänzungen sind u.a. in [VDI/VDE 3681] und [Chouikha et al. 2000] zu finden.

Die Vorteile der Anwendung formaler Techniken bezüglich einer präzisen, nachvollziehbaren und qualitätsgerechten Entwicklung wurden hinlänglich erläutert [Schnieder 1999]. Entscheidend für eine erfolgreiche Anwendung ist dabei die Durchgängigkeit vor allem des Beschreibungsmittels. Unter Zuhilfenahme verschiedener Beschreibungsmittel werden Transformationen durch den Bearbeiter oder durch zusätzliche Werkzeuge erforderlich, welche zu Fehlern bzw. Inkonsistenzen führen können. Die Anzahl der in der Methode verwendeten Beschreibungsmittel ist korrelierend mit dem Fehlerpotenzial, wodurch eine zahlenmäßige Einschränkung sinnvoll ist.

Mittels der formalen Technik ist in einer Risikoanalyse für ein sicherheitsrelevantes System das auftretende Risiko zu quantifizieren. Bei der Analyse ist das System rein funktional und aus

betrieblicher Sicht zu betrachten, technische Realisierungen bleiben dabei unberücksichtigt. Beginnend mit der Systemdefinition werden die funktionalen Anforderungen des Systems festgelegt. Der eigentliche betriebliche Prozess wird dabei bereits berücksichtigt und alle betriebsbezogenen Systemparameter herangezogen. Durch Analyse der Interaktionen des Systems mit dem betrieblichen Prozess werden potenzielle Gefährdungen mittels formaler Vorgehensweise identifiziert, wobei u.a. das PROFUND-Konzept [Slovak 2007] Anwendung finden kann. Das resultierende Risiko aus den potenziell gefährlichen Situationen wird anschließend formal quantifiziert und den systembezogenen Ursachen geeignet begegnet. Als finales Ergebnis der Risikoanalyse werden abschließend die funktionalen, systembezogen tolerierbaren Gefährdungsraten (THR) als quantitativ funktionale Sicherheitsziele zum resultierenden betrieblichen Risiko in Beziehung gesetzt und unter Zuhilfenahme eines geeigneten Risikoakzeptanzkriteriums (GAMAB, ALARP, MEM etc.) nach [EN 50126] abgeleitet.

4.2.1.1 Petrinetze

Nach ihrem Erfinder Carl Adam Petri benannt, sind Petrinetze ebenso wie Zustandsübergangsdiagramme Modelle, mit denen Systemzustände sowie deren Übergänge aufgrund von Ereignissen modelliert werden können. Insbesondere eignen sich Petrinetze für Modellierungen paralleler oder verteilter Systeme, welche aus Teilsystemen bestehen, deren Zustand sich unabhängig weiterentwickelt. Als normative Grundlage für Petrinetze ist die IEC 62551 zu nennen. Kanal-Instanzen Netze gehören zu den untergeordneten Petrinetzen (low-level Netze). Sie bestehen aus Stellen und Übergängen bzw. Transitionen, welche durch gerichtete Kanten verbunden sind. Direkte Verbindungen zwischen zwei Stellen oder zwei Transitionen bestehen nicht. Bei der Modellbildung werden Stellen in Form von Kreisen, Transitionen als Rechtecke und Kanten als Pfeile dargestellt. Bei einem aktiven Zustand einer Stelle wird diese mit Hilfe eines Tokens markiert. Eine vertiefende Unterscheidung und Modellierungsgrundlagen von Petrinetzen ist u.a. in [Schnieder 1999] und [Drewes 2009] zu finden.

4.2.1.2 Ereignisbaumanalyse

Die Ereignisbaumanalyse (Event Tree Analysis) ist eine Methode, mit der mögliche Folgen eines auftretenden Systemfehlers bestimmt werden können. Bei der Ereignisbaumanalyse wird ein Ereignis (Zustandsübergang), das in einem System auftreten kann, und dessen mögliche Auswirkungen auf das Gesamtsystem untersucht. Die Wirkung des auslösenden Ereignisses wird unter normalen Betriebsbedingungen und unter der Annahme, dass das nachfolgende Teilsystem fehlerhaft ist, betrachtet. Als Ergebnis wird ein binärer Baum üblicherweise von links nach rechts erstellt, der an jeder Abzweigung zwei Alternative bietet. Der obere Zweig stellt das erfolgreiche Verhalten als Ereignisfolge dar, während der untere Zweig das Versagen darstellt. In Kombination mit Zahlenwerten sind Unfallwahrscheinlichkeiten zu berechnen. Ein Nachteil der Methode ist die Verdopplung der Betrachtungsschritte je abzweig, wodurch die Betrachtung komplexer Systeme sehr unübersichtlich werden kann. Als normative Grundlage ist die DIN 25419 mit weiteren Details heranzuziehen.

4.2.1.3 Störungsbaumanalyse

Die Störungs- oder Fehlerbaumanalyse (Fault Tree Analysis) stellt eine Methode dar, um die Wahrscheinlichkeit eines Systemausfalls zu bestimmen. Die für sämtliche Systeme geeignete Analyse impliziert ein unerwünschtes Ereignis und lässt in systematischer Weise in Form einer Baumstruktur (top down) die Suche nach allen kritischen Pfaden zu, welche das unerwünschte Ereignis auslösen können. Als normative Grundlage ist die DIN 254124 mit weiteren Details heranzuziehen.

4.2.1.4 Markov-Modelle

Ein Markov-Modell (auch Markov-Kette genannt) ist ein Prozessmodell mit globalen Systemzuständen und deren stochastischer Bewertbarkeit. Wahrscheinlichkeiten für das Eintreten zukünftiger Ereignisse anzugeben ist die Zielstellung der Modellbildung. Die hervorzuhebende Eigenschaft des Markov-Modells ist, dass durch Kenntnis weniger globaler Vorzustände des Systems geeignete Prognosen über die Prozess- und Systementwicklung möglich sind. Als normative Grundlage ist die IEC 61165 mit weiteren Details heranzuziehen.

4.2.1.5 FME(C)A

Bei der Betrachtung der Ursachen und Folgen in Verbindung mit potenziellen Systemgefährdungen hat sich die Anwendung der FMEA (Failure Mode and Effects Analysis / Fehlermöglichkeits- und Einflussanalyse) bzw. der FMECA (Failure Mode and Effects and Criticality Analysis) als geeignete Methode nach [EN 60812] erwiesen und in der Fachwelt etabliert.

Bereits 1980 wurde die FMEA als Ausfalleffektanalyse in die DIN 25448 aufgenommen, die im Jahr 2006 durch DIN EN 60812 ersetzt wurde. Die FMEA folgt dem Grundgedanken einer vorsorgenden Fehlerverhütung anstelle einer nachsorgenden Fehlererkennung und -korrektur (Fehlerbewältigung) durch frühzeitige Identifikation potenzieller Fehlerursachen bereits in der Entwurfsphase des V-Modells. Damit werden ggf. anfallende Kontroll- und Fehlerfolgekosten in späteren Produktlebensphasen gering gehalten und die Kosten insgesamt gesenkt. Durch die systematische Vorgehensweise und die dabei gewonnenen Erkenntnisse kann außerdem die Wiederholung von Entwicklungsmängeln bei neuen Produkten und Prozessen entsprechend der Qualitätsmanagementphilosophie vermieden werden [FMEA 2006].

Grundarten der FME(C)A

- System-FMEA: Diese untersucht das Zusammenwirken von Teilsystemen in einem übergeordneten Systemverbund bzw. das Zusammenwirken mehrerer Komponenten in einem komplexen System. Sie zielt dabei auf die Identifikation potenzieller Schwachstellen – insbesondere auch an den Kontaktstellen – ab, die durch das Zusammenwirken der einzelnen Komponenten oder die Interaktion des eigenen Systems mit der Umwelt entstehen könnten. Die System-FMEA wird innerhalb des Entwicklungsprozesses für ein Produkt angewendet. Ihre Aufgabe ist es, das Produkt auf Erfüllung der im Pflichtenheft festgelegten Funktionen hin zu untersuchen. Dabei sind für alle risikobehafteten Teile eines Produktes geeignete Maßnahmen zur Vermeidung oder Entdeckung der potenziellen Fehler zu planen.
- Konstruktions-FMEA: Diese untersucht die Konstruktion einzelner Bauteile oder Komponenten und prüft diese auf potenzielle Schwachstellen oder Ausfallmöglichkeiten.

Ergänzende Arten der FME(C)A

- Prozess-FME(C)A: Diese stützt sich auf die Ergebnisse der Konstruktions-FMEA und befasst sich mit möglichen Schwachstellen im Fertigungs- oder Leistungsprozess.
- Hardware-FME(C)A: Diese hat zum Ziel, Risiken aus dem Bereich Hardware und Elektronik zu analysieren, zu bewerten und mit Maßnahmen abzustellen.
- Software-FME(C)A: Diese leistet dieselbe Aufgabe wie die Hardware-FME(C)A für den erzeugten Programmcode.

Folgende Bestandteile sind in der FME(C)A enthalten und bei der Analyse zu berücksichtigen:

- eine Eingrenzung des betrachteten Systems,
- eine analytische Strukturierung des betrachteten Systems,
- die Definitionen von Funktionen der Strukturelemente,
- eine Prüfung auf potenzielle Fehlerursachen, -arten und -folgen, die sich direkt aus den Funktionen der Strukturelemente ableiten,
- eine erste Risikobeurteilung,
- Maßnahmen- bzw. Lösungsvorschläge zu priorisierten Risiken,
- eine Verfolgung vereinbarter Vermeidungs- und Entdeckungsmaßnahmen und
- eine Restrisikobeurteilung bzw. -bewertung.

In der Erweiterung werden potenzielle Systemfehler in der FMECA analysiert, indem die Fehlerfunktion bzw. die Fehlerkomponente lokalisiert, die Fehlerart bestimmt, die Fehlerfolge beschrieben und anschließend die Fehlerursache ermittelt wird. Kennzahlen zur Bedeutung (*B*) der

Fehlerfolge, zur Auftretenswahrscheinlichkeit (*A*) der Fehlerursache und zur Entdeckungswahrscheinlichkeit (*E*) des Fehlers oder seiner Ursache stellen die Grundlage für eine quantitative Risikobewertung dar.

Die Kennzahlen sind ganzzahlige Werte zwischen 1 und 10 und werden projektbezogen nach folgender Bewertung vergeben.

- (*B*) Bedeutung der Fehlerfolge aus Anwendersicht (gering = 1, hoch = 10)
- (*A*) Auftretenswahrscheinlichkeit der Fehlerursache (gering = 1, hoch = 10)
- (*E*) Entdeckungswahrscheinlichkeit des Fehlers (hoch = 1, gering = 10)

4.2.2 Abschätzung des Risikos

Mittels der FMECA kann ein potenzielles Risiko für einen betrachteten Betriebsprozess mitsamt den zugehörigen Ursachen quantitativ analysiert werden. In einer ersten Bewertung kann unter Berücksichtigung der Risikoprioritätszahl die Wahrscheinlichkeit des Auftretens und die Auswirkung einer Gefährdung herausgestellt werden.

Ab einer abgeschätzten Risikoprioritätszahl > 50 – die Basis wird entsprechend der jeweiligen Sicherheitsphilosophie (des Unternehmens) bzw. als Bestandteil der Sicherheitskultur des Unternehmens festgelegt – werden dann potenzielle Fehler und Folgen näher betrachtet [Braband 2005]. Darunterliegende Werte (< 50) stellen für eine weitere Betrachtung i.d.R. keine Bedeutung dar, da jedes technische Produkt und jeder technische Prozess ein Grundrisiko besitzt.

Genauer untersucht und quantitativ bewertet werden dabei:

- die Einschätzung des möglichen Risikos
- die zu treffenden Maßnahmen zur Eingrenzung des Risikos
- die Häufigkeit des Auftretens der Gefährdung
- der Schweregrad und die Konsequenzen des Auftretens

Abschließend kann eine Einstufung der Risiken in die Risikomatrix nach DIN EN 50126 erfolgen (vgl. Bild 4.7).

Den eingestuften Risiken muss bei der Umsetzung des Systems durch Risikoreduktionen begegnet werden. Eine Nachweisführung gegen Risikoakzeptanzkriterien schließt sich an.

4.2.3 Bewertung von Risiken

Um das jeweilige Risiko einer Systemfunktion, im Kontext zu einem Betriebsprozess, abschließend bewerten zu können, kann die Risikomatrix nach EN 50126 mit der Einteilung in qualitative Risikokategorien herangezogen werden (Bild 4.7).

Häufigkeit von Gefahrenfällen	**Risikobewertung**			
häufig	*unerwünscht*	*intolerabel*	*intolerabel*	*intolerabel*
wahrscheinlich	*tolerabel*	*unerwünscht*	*intolerabel*	*intolerabel*
gelegentlich	*tolerabel*	*unerwünscht*	*unerwünscht*	*intolerabel*
selten	*vernachlässigbar*	*tolerabel*	*unerwünscht*	*unerwünscht*
unwahrscheinlich	*vernachlässigbar*	*vernachlässigbar*	*tolerabel*	*unerwünscht*
unvorstellbar	*vernachlässigbar*	*vernachlässigbar*	*vernachlässigbar*	*tolerabel*
	unbedeutend	**marginal**	**kritisch**	**katastrophal**
	Gefahrenstufen			

Bild 4.7: Risikomatrix (Häufigkeits-Konsequenz-Matrix) nach [EN 50126]

Die qualitative Einstufung der Risikobewertung lässt unter Berücksichtigung der Risikoabschätzung folgende Risikokategorien zu, durch die sich das Risiko der identifizierten Gefährdungen bewerten lassen (Bild 4.8). Über die Quantifizierung der Kategorien werden in der Norm keine Aussagen getroffen, da diese nach der jeweiligen Sicherheitsphilosophie des Anwenders bzw. des Eisenbahnunternehmens (EVU / EIU) einzustufen sind.

Risikokategorie	Anzuwendende Maßnahme
intolerabel	Muss ausgeschlossen werden.
unerwünscht	Darf nur akzeptiert werden, wenn eine Risikominderung praktisch nicht durchführbar ist und eine Zustimmung entweder des Bahnunternehmens oder der für die Sicherheit zuständigen Aufsichtsbehörde vorliegt.
tolerabel	Akzeptierbar bei geeigneter Überwachung und mit der Zustimmung des Bahnunternehmens.
vernachlässigbar	Akzeptierbar auch ohne weitere Zustimmung des Bahnunternehmens.

Bild 4.8: Qualitative Risikokategorien nach [EN 50126]

4.2.4 Risikoquantifizierung

Bereits in Bild 4.7 wird deutlich, dass sich zwischen der vernachlässigbaren und der tolerierbaren Risikokategorie das Grenzrisiko in eine gedachte Linie bzw. einem gedachten Band projizieren lässt, welches in Abhängigkeit des zugrunde gelegten Risikoakzeptanzkriteriums steht. Dieses „gedachte Band“ kann bei einer möglichen semiquantitativen Einstufung mit Hilfe der Risikoprioritätszahl (RPZ) aus den Ergebnissen der FMECA bewertet werden.

Mit der Berechnung der RPZ wird eine Rangfolge der Systemrisiken erstellt, die in einer Risikoskalierung eingepasst werden kann, wodurch wiederum das Grenzrisiko spezifisch anpassbar ist. Die RPZ berechnet sich durch Multiplikation der B-, A- und E-Faktoren:

$$RPZ = B \cdot A \cdot E \tag{4.1}$$

und kann entsprechend diskrete Werte zwischen 1 und 1.000 annehmen (vgl. Abschnitt 4.2.1). Es besteht der Anspruch, dass die RPZ – mindestens im Vergleich mit anderen RPZ der gleichen FMECA – eine Aussage im Sinne besser oder schlechter erlaubt [FMEA 2006]. Aufgrund der multiplikationsbedingten Streuung der Werte im unteren Bereich, erscheint der statische Ansatz, einen Grenzwert bei RPZ = 50 anzunehmen als zielführend. Das beherrschbare Risiko wird somit hier mit dem Zahlenwert 50 quantifiziert, wodurch die Annahme zugrunde gelegt wird, dass bei einer mittleren Bedeutung der Fehlerfolge ($B < 5$) und maximal mittleren Auftretenswahrscheinlichkeit ($A < 5$) eine hohe Entdeckungswahrscheinlichkeit angenommen wird.

Ein weiterer Grenzwert wird bei der RPZ = 125 angenommen. Bei Ergebnissen oberhalb dieses Wertes sind zwingend geeignete Abstellmaßnahmen festzulegen und deren Bearbeitung und Ergebnisse zu protokollieren. Der Grenzwert von 125 setzt sich aus der Annahme zusammen, dass alle Bereiche maximal mittlere Werte annehmen:

$$125 = \mathrm{RPZ} = B \cdot A \cdot E = 5 \cdot 5 \cdot 5$$

Im Bereich zwischen 50 und 125 sind als Maßnahmen Risiken, Chancen und Aufwand sachkundig abzuwägen.

Andere Ansätze durch z.B. Addition oder durch Logarithmieren der RPZ-Parameter sind in [Braband 2005] erläutert, sollen an dieser Stelle aber nicht weiter verfolgt werden.

Nach der absoluten Berechnung der RPZ zielen anschließende Maßnahmen darauf ab, die Auftretenswahrscheinlichkeit einer Fehlerursache zu reduzieren (z.B. durch Empfehlung von Redundanzen) sowie die Entdeckungswahrscheinlichkeit für potenzielle Fehlerursachen zu erhöhen (z.B. durch zusätzliche Prüfungen der Systemkomponenten), wodurch in einer Iteration der Wert der RPZ in den sicheren Bereich reduziert wird [FMEA 2006].

4.3 Zuverlässigkeitsbetrachtung

Die Zuverlässigkeit (R – Reliability) ist eine Eigenschaft eines technischen Systems. Innerhalb eines vorgegebenen Zeitintervalls muss ein Produkt seine Funktionalität erfüllen. Die Zuverlässigkeit kann mittels stochastischer Prozesse quantitativ ermittelt werden. Die Zuverlässigkeit eines Teilsystems wird durch empirische Ermittlung der Ausfallhäufigkeit oder mittels analytischer Ableitung der mittleren Ausfallraten der Teilsystemkomponenten bestimmt. Die Zuverlässigkeit sämtlicher Teilsysteme und -prozesse führt zur Verfügbarkeit des Gesamtsystems. Die Verfügbarkeit eines Systems ist somit nur in Abhängigkeit der Zuverlässigkeitswerte der Systemkomponenten zu betrachten [Bertsche 2004].

4.4 Verfügbarkeitsbetrachtung

Verfügbarkeit als Eigenschaft eines Systems wird als die Fähigkeit eines Produkts oder Systems definiert, sich in einem Zustand zu befinden, in dem es unter vorgegebenen Bedingungen zu einem vorgegebenen Zeitpunkt oder während einer vorgegebenen Zeitspanne eine geforderte Funktion unter der Voraussetzung erfüllen kann, dass alle geforderten äußeren Hilfsmittel bereitstehen [EN 50126]. Somit ist ein z.B. ein sicherheitsrelevantes Ortungssystem dann verfügbar, wenn es eine Ortsinformation unter sicherheitsrelevanten Aspekten zu den vorgegebenen Zeitpunkten einem übergeordneten System zur Verfügung stellt. Berechnet wird die Verfügbarkeit (A) durch:

$$A = \frac{MUT}{MUT + MDT} \tag{4.2}$$

Als *MUT* (mean up time) wird die mittlere Zeit zwischen zwei Ausfällen bezeichnet und mit *MDT* (mean down time) die mittlere Zeit in der das System nach erkanntem Ausfall nicht zur Verfügung steht (Unverfügbarkeit). Die Unverfügbarkeit kann wiederum in eine geplante als Instandhaltung ($1 - A_M$) sowie eine ungeplante als Reparatur ($1 - A_R$) unterteilt werden. Wird ein System somit häufiger durch Instandhaltung geplant unverfügbar, sinkt die Wahrscheinlichkeit einer ungewollten Unverfügbarkeit, wodurch das System zwar insgesamt weniger verfügbar, in der Sicherheitsbetrachtung aber sicherer wird [Braband 2005].

4.5 Instandhaltungsbetrachtung

Die Instandhaltung (M – Maintenance) stellt den ergänzenden Zusammenhang zwischen der Sicherheit und der Verfügbarkeit dar und umfasst einerseits die Möglichkeit, ein Produkt oder System überhaupt instand zu halten sowie andererseits den Aufwand, der betrieben werden muss, um das System so zu überprüfen, dass es seine Funktionalität beibehält. Daraus wird ersichtlich, dass die Instandhaltung die Lebenszykluskosten eines Systems stark beeinflusst [EN 50126].

4.6 Integration von Verfügbarkeit und Sicherheit

Zwischen den globalen Zustandseigenschaften Sicherheit und Verfügbarkeit technischer Systeme besteht unter Berücksichtigung der Instandhaltung der Systemkomponenten und deren jeweiliger Zuverlässigkeit ein Zusammenhang [Schnieder 2009]. Ein im Betrieb befindliches System führt die bestimmten Funktionen im Regelfall sicher aus, und die Gesamtverfügbarkeit ist damit gewährleistet. Ein Ausfall einer Systemkomponente kann sich verfügbarkeitsrelevant auswirken, wodurch das System in einen sicheren, aber unverfügbaren Zustand überführt wird. Im anderen Fall kann sich bei sicherheitsrelevanten Systemen ein Komponentenausfall auch sicherheitsrelevant auswirken; durch redundante Sicherungsfunktionen, welche in der Sicherheitsuntersuchung betrachtet werden, kann in der Regel nur ein gefährlicher Systembetrieb als Zustand erreicht werden, der sich bei einem zusätzlichen Komponentenausfall zu einem Gesamtsystemausfall mit einem Schaden entwickeln kann. Die jeweiligen vorgelagerten globalen Zustände sind über Reparaturen zu erreichen. Dieser zusammenhängende Sachverhalt ist in Bild 4.9 wiedergegeben [Schnieder 2003].

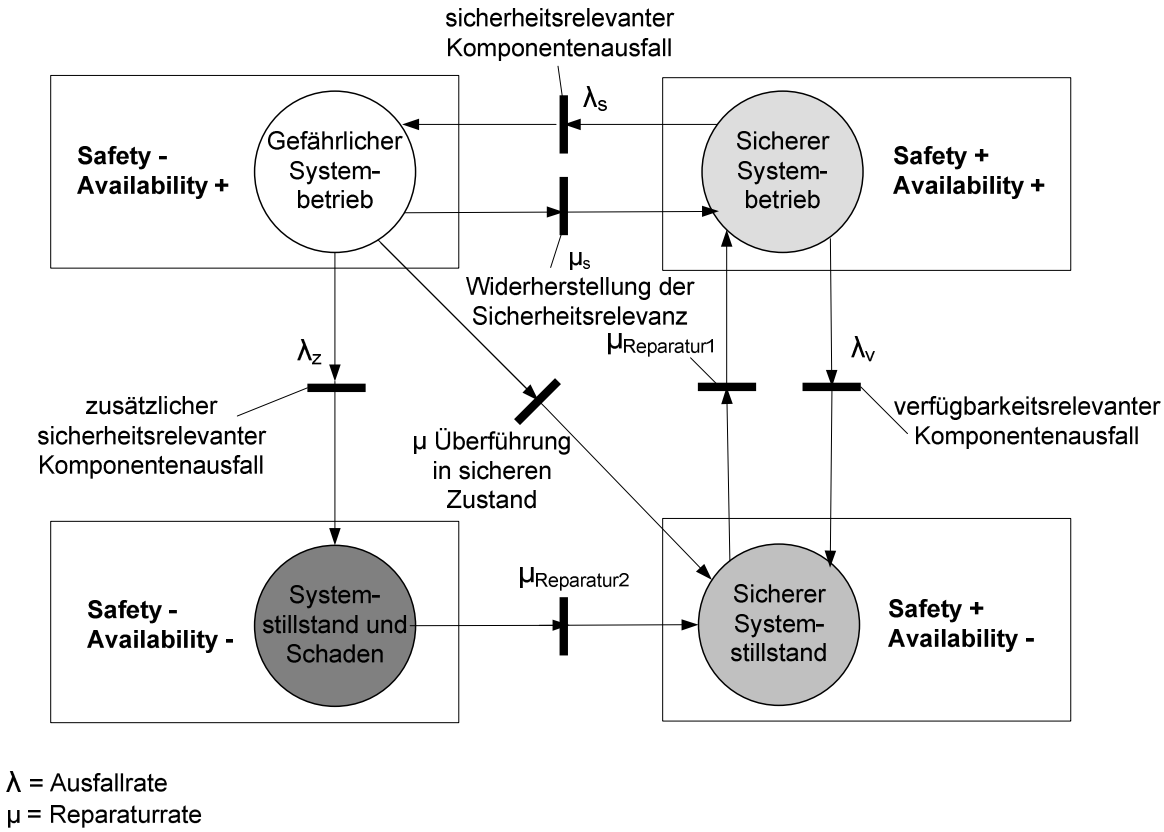

Bild 4.9: Globale Systemzustände der Verlässlichkeit und lokale Zustandsübergänge der Zuverlässigkeit und Instandhaltbarkeit von Komponenten, nach [Schnieder 2003]

Wie aus Bild 4.9 ersichtlich, lässt sich der Zusammenhang zwischen Sicherheit und Verfügbarkeit in vier Quadranten darstellen. Dies kann in ein Sicherheits- und Verfügbarkeitsdiagramm integriert

werden, bei dem in horizontaler Richtung die Sicherheit, in vertikaler Richtung die Verfügbarkeit aufgetragen und quantifiziert wird (Bild 4.10).

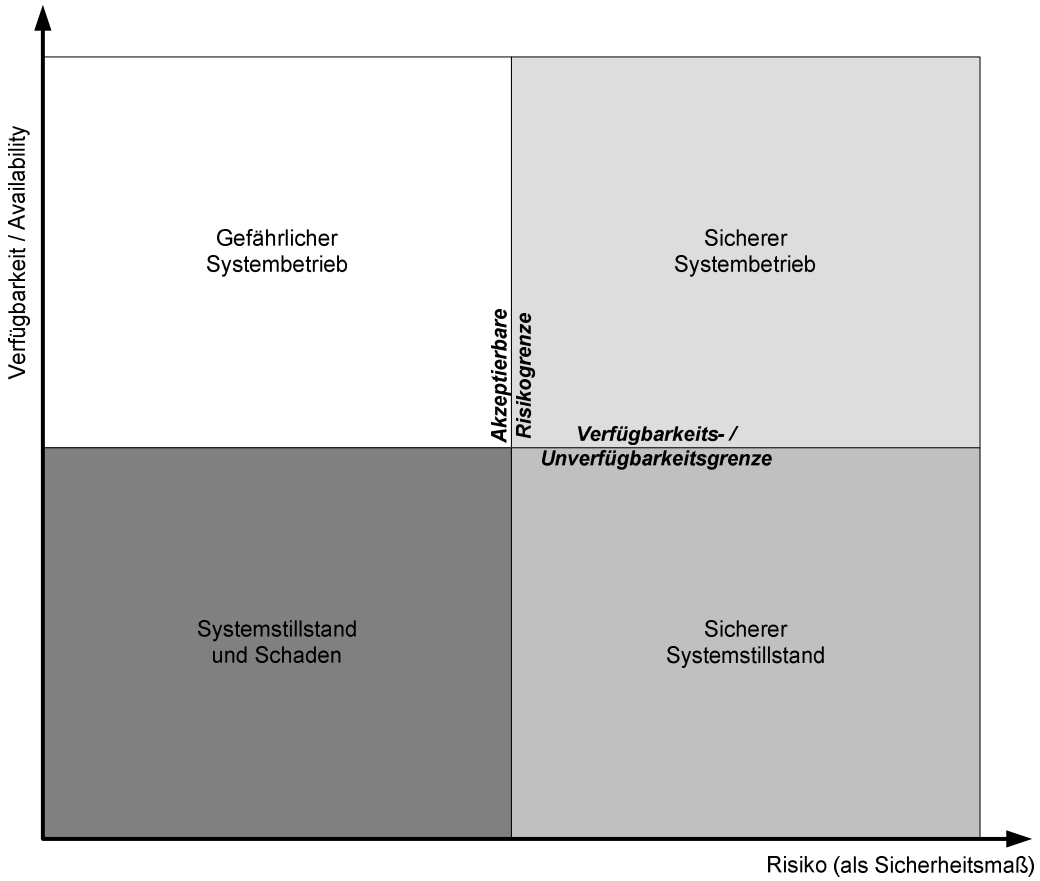

Bild 4.10: Sicherheits- und Verfügbarkeitsdiagramm, nach [Schnieder 2003]

Dem vorliegenden rein qualitativen Diagramm können für eine Quantifizierung Maße (Größen) der Sicherheit in Form des Risikos mit Werteangaben durch z.B. Risikoprioritätszahlen im Bereich zwischen 0 und 1.000 zugeordnet werden. Der Verfügbarkeit kann der maximale Wert 1 (100 %) angetragen werden; an der Verfügbarkeits-/Unverfügbarkeitsgrenze wird als Übergangswert beispielhaft eine Verfügbarkeit von 0,99 angesetzt. Die vier Quadranten werden durch qualitative Begrenzungen des Grenzrisikos sowie durch den Übergang zwischen Verfügbar- und Unverfügbarkeit unterteilt, wobei diese Grenzen sehr stark von der jeweiligen Sicherheitskultur und -philosophie der am jeweiligen Untersuchungsprojekt beteiligen Institutionen abhängen [Schnieder 2003].

5 DURCHGÄNGIGE METHODE ZUR SICHERHEITSUNTERSUCHUNG

Unter Berücksichtigung der methodischen Grundlagen aus Kapitel 4 wird nachfolgend eine durchgängige Methode zur praktischen Anwendbarkeit von Sicherheitsuntersuchungen vorgestellt. Bei der Sicherheitsuntersuchung wird in Abgrenzung zur Sicherheitsanalyse auch der den gesamten Lebenszyklus begleitende Sicherheitsnachweis mit einbezogen (vgl. Definitionen Abschnitt 4.1).

5.1 Konzeptioneller Ansatz

Basis aller Verlässlichkeitsbetrachtungen (RAMS) im Schienenverkehr und Betrachtungsgegenstand der Methode sind die Kommunikationswege, welche grundsätzlich automatisiert umgesetzt werden können. Jede Kommunikation mit der Übersendung von Informationen kann auf Seiten des Versenders, auf Seiten des Empfängers, bei der Übermittlung oder durch Unterlassung und Unvollständigkeit zu Fehlern führen, die entsprechend negative Auswirkungen nach sich ziehen.

Durch den Ersatz von menschlicher Kommunikation durch technische Datenübertragung können Fehler auf die technische Zuverlässigkeit der Teilkomponenten oder -systeme eingegrenzt werden. Als innovativer Ansatz für die Offenbarung von Gefährdungen ist daher die Betrachtung der Informationsübertragung über Kontaktstellen menschlicher und technischer Systeme erforderlich. Bild 5.1 verdeutlicht exemplarisch den Sachverhalt am Kommunikationsbeispiel zwischen einem Eisenbahnfahrzeugführer und einem Zugleiter: Bei jeder Informationsübertragung und -verarbeitung können Fehler entstehen, die als potenzielle Gefährdungen untersucht werden müssen.

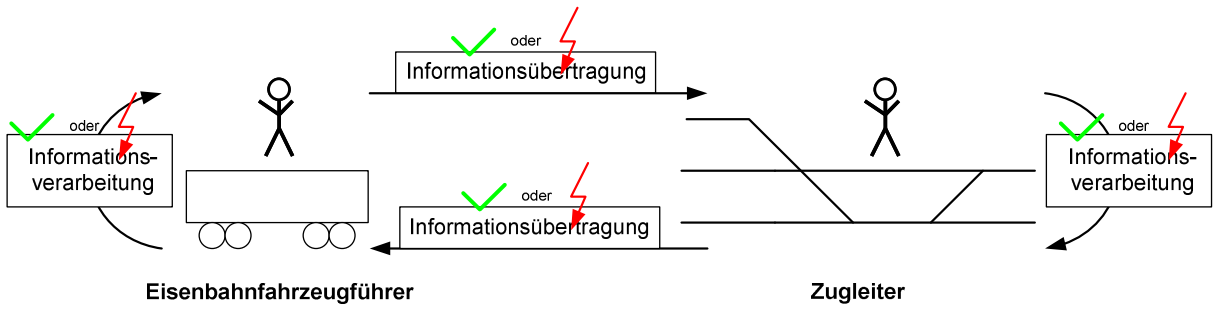

Bild 5.1: Fehlerpotenziale durch (menschliche) Kommunikation

Die normkonforme Bearbeitung der Sicherheitsuntersuchung erfordert eine ganzheitliche dokumentarische Begleitung des Systems in allen Phasen des V-Modells.

Bei der Erstellung einer durchgängigen Sicherheitsuntersuchung treten nachstehende Fragen auf, die es zu beantworten gilt:

- Wie lässt sich das zu betrachtende System abgrenzen?
- Welche Funktionen können abgeleitet werden?
- Welches sind Sicherheitsfunktionen und welches betriebliche Funktionen?
- Welche Systemkomponenten sind bei der Untersuchung entscheidend?
- Bis zu welcher Systemtiefe sind qualitative und quantitative Aussagen erhältlich?
- Welche Richtlinien und Standards sind anzuwenden?
- Wie sicher ist sicher?
- Welches Grenzrisiko kann als akzeptierbar angenommen werden?
- Wie sind Sicherheitsphilosophie und -kultur des Unternehmens ausgeprägt?
- Reichen Verweise bei der Dokumentation aus oder muss ausformuliert werden?

Aufgrund der Festlegung, dass ein technisches System, z.B. das Ortungssystem, Sicherheitsverantwortung trägt, sind entsprechend für das System Sicherheitsanforderungen aufzustellen, welche im begleitenden Sicherheitsnachweis nachgewiesen werden. Nach der deutschen Eisenbahn-Bau- und Betriebsordnung (EBO) §2 (2) wird für ein zusätzliches System der Nachweis mindestens gleicher Sicherheit gefordert. Die Sicherheit, die ein bestehendes vergleichbares System erreicht, muss ein neues System gleicher Funktionalität mindestens erfüllen. Bezugsgröße ist dabei der jeweilige Betrachtungsfall, d.h. die zu betrachtende Strecke oder das auszurüstende Fahrzeug [EBO 2008].

Für das Konzept einer Sicherheitsuntersuchung stellt Bild 5.2 die Inhalte der Sicherheitsanalyse entsprechend der DIN EN 50126 in Verbindung mit Bild 4.4 vor. Im Rahmen einer Risikoanalyse sind eine Systemdefinition, eine Gefährdungsidentifikation, eine Ursachen- und Folgenanalyse sowie eine Risikoabschätzung zu erarbeiten [EN 50126].

Nach Festlegung einer tolerierbaren Gefährdungsrate (THR) wird im Rahmen einer Gefährdungsanalyse die Beherrschung der Gefährdungen erarbeitet.

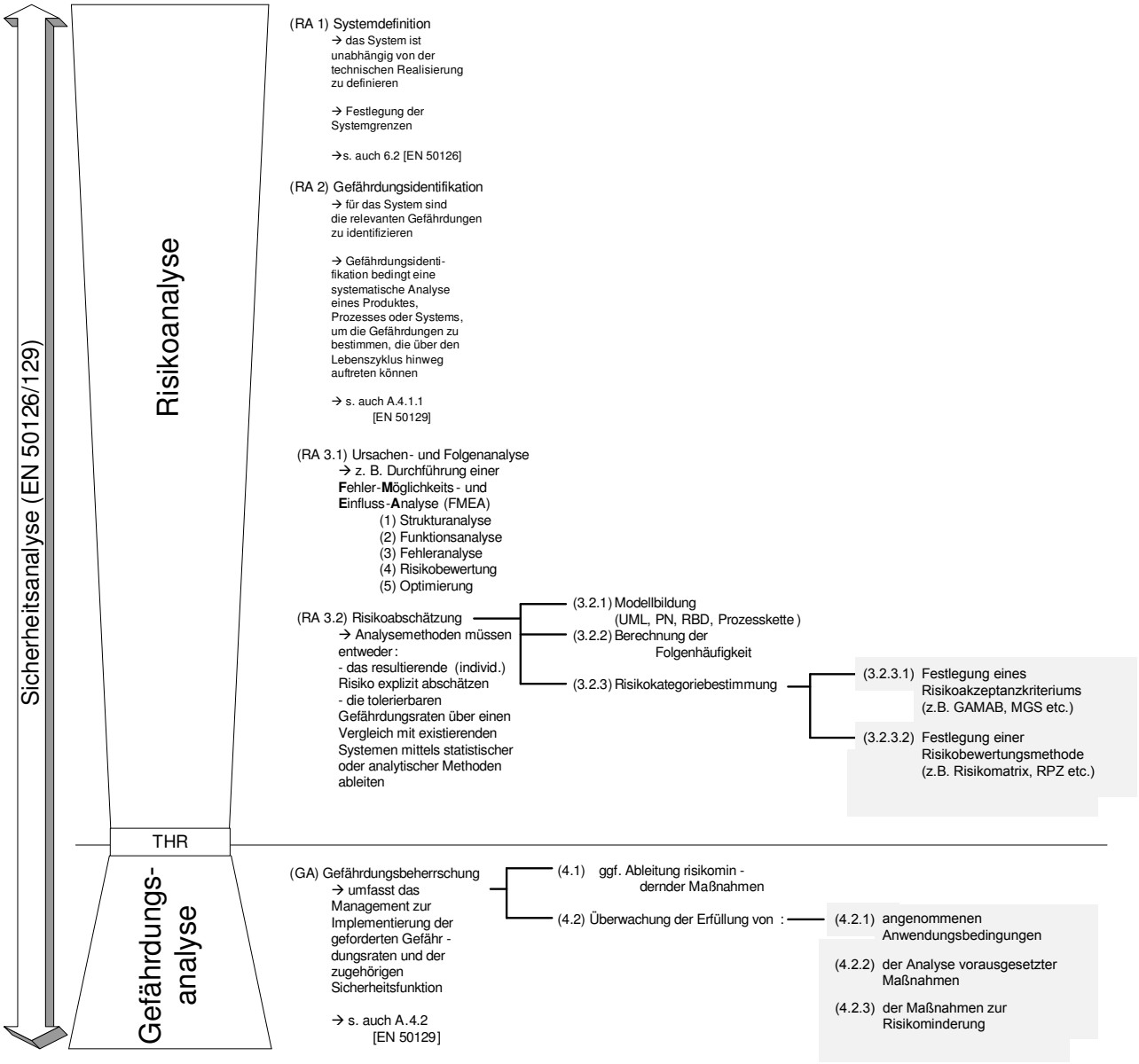

Bild 5.2: Arbeitsinhalte einer Sicherheitsanalyse

Wird abschließend der Zusammenhang zwischen einer Sicherheitsanalyse und dem Sicherheitsnachweis betrachtet, lässt sich ableiten, dass der Sicherheitsnachweis als ein letztendlicher Vergleich der Sicherheitsanforderungen aus der Sicherheitsanalyse des „neuen“ Systems mit Referenzergebnissen eines bereits existierenden, in Betrieb befindlichen „alten“ Systems herangezogen werden kann. Dadurch kann die Forderung des Nachweises mindestens gleicher Sicherheit durch geeigneten kombinierten Einsatz von Sicherheitsanalyse und -nachweis erfüllt werden.

5.2 Methodischer Ansatz

Der methodische Ansatz für eine Sicherheitsuntersuchung wird in diesem Abschnitt nach Sicherheitsanalyse und Sicherheitsnachweis untergliedert vorgestellt.

5.2.1 Sicherheitsanalyse

Aus den Betrachtungen der vorhergehenden Abschnitte (vgl. Bild 5.2) lässt sich das Vorgehen für die Entwicklung einer Methode herausarbeiten. Im ersten Schritt sind das Betrachtungssystem einzugrenzen und relevante Funktionen abzuleiten. Die Systemteile sind zu analysieren und festzulegen, wodurch eine ganzheitliche Systemdefinition nach DIN EN 50126 gegeben ist. In der hier vorgestellten Methode wird mittels Kanal-Instanzen-Netzen [Schnieder 1999] anschließend die Definition der mit dem System im Zusammenhang stehenden Betriebsprozesse aufgestellt, wodurch Rückschlüsse auf die zu betrachtende Systemtiefe für spätere qualitative als auch quantitative Aussagen gezogen werden können. Ein gesondertes Werkzeug ist dafür nicht erforderlich. Die definierten Prozesse werden als Grundlage für die Gefährdungsidentifikation verwendet. Als Referenz, insbesondere zur Erlangung einer maximalen Vollständigkeit wird – sofern verfügbar – eine Gefährdungsliste (Hazard-List) bzw. generiert aus einer Gefährdungstabelle herangezogen, die ggf. allgemeingültige Sicherheitsanforderungen liefert. Die herausgearbeiteten Gefährdungen werden mit Hilfe einer Failure-Mode-and-Effect-Analysis (FMEA) [EN 60812] anschließend einer qualitativen Ursachen- und Folgenanalyse mit Berücksichtigung quantitativer Ansätze unterzogen. Als geeignetes Werkzeug kann hierbei MS-Excel eingesetzt werden. Eine quantitative Risikoabschätzung unter Berücksichtigung der Risikomatrix nach DIN EN 50126 und Festlegung eines akzeptierbaren Risikos wird durch eine FME(C)A (Failure-Mode-Effect-and-Criticality-Analysis) umgesetzt. Durch abschließenden Vergleich wird die Risikobewertung des Systems durch Gegenüberstellung mit einem Referenzsystem entsprechend EBO §2 (2) durchgeführt und die Beherrschung der potenziellen Systemgefährdungen diskutiert. Eine Plausibilisierung der Risikoreduktionsfaktoren schließt sich an [2009/352/EG 2009].

Der kausale Zusammenhang des methodischen Konzepts zur Sicherheitsuntersuchung wird in Bild 5.3 verdeutlicht.

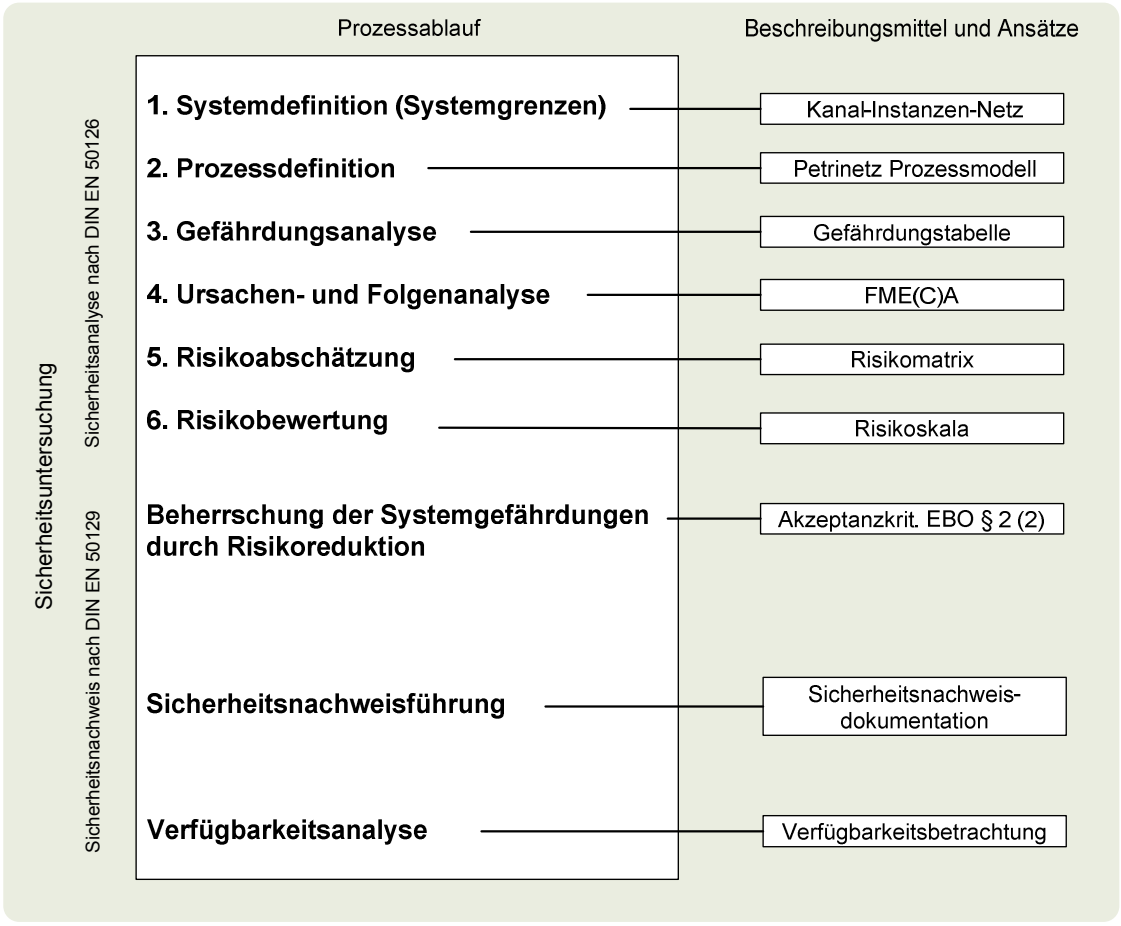

Bild 5.3: Generische Methodenstruktur zur Sicherheitsuntersuchung inkl. zugehöriger Beschreibungsmittel

5.2.1.1 Systemdefinition

Das System, auf das sich die Sicherheitsanalyse bezieht, ist genau zu definieren. Dabei sind mindestens die folgenden Aspekte zu berücksichtigen:

- Funktionalität und Nutzungszustände
- Wirkbereich und Abgrenzungen
- Systemarchitektur

Nach [EN 50129] ist die Systemdefinition auch Inhalt des technischen Sicherheitsberichts, wodurch ein Verweis auf diesen erfolgen kann.

5.2.1.2 Prozessdefinition

Ergänzend zum betrachteten System wird an dieser Stelle der zu untersuchende Betriebsprozess definiert. Um den Prozess geeignet zu identifizieren und zu beschreiben, ist als methodisches Vorgehen seine Einordnung in einem Regelkreis sinnvoll [Drewes/May 2007]. Ein kontinuierlicher Betriebsprozess wird in diesem Fall als Regelkreis aufgesetzt, wobei als Entscheidungsbasis Regeln und Zielvorgaben den personellen (z.B. Zug- bzw. Eisenbahnfahrzeugführer und Zugleiter) sowie technischen Ressourcen zur Verfügung stehen und umgesetzt werden müssen. Generisch gesehen ermitteln die Ressourcen Informationen, werten diese aus und übertragen sie in geeigneter Form an andere Ressourcen, bei denen eine Umwandlung der Information zu einem Ergebnis bzw. zu einer Aufgabe wird, die dann wiederum in Form einer Meldung zurück übertragen werden kann. In welcher Form die Übertragung stattfindet, ist dabei unerheblich. Entscheidend für die weitere Bearbeitung ist, dass in jedem Prozessschritt potenzielle Fehler durch falsche Interpretation (Ermittlung oder Verarbeitung) der Daten oder der Übertragung selbst entstehen können (vgl. Bild 5.1).

Bild 5.4 stellt am Beispiel des Zugleitbetriebs den generischen Regelkreis eines Eisenbahnbetriebsprozesses mit den Kommunikationsebenen zwischen Zug- bzw. Eisenbahnfahrzeugführer und Zugleiter dar.

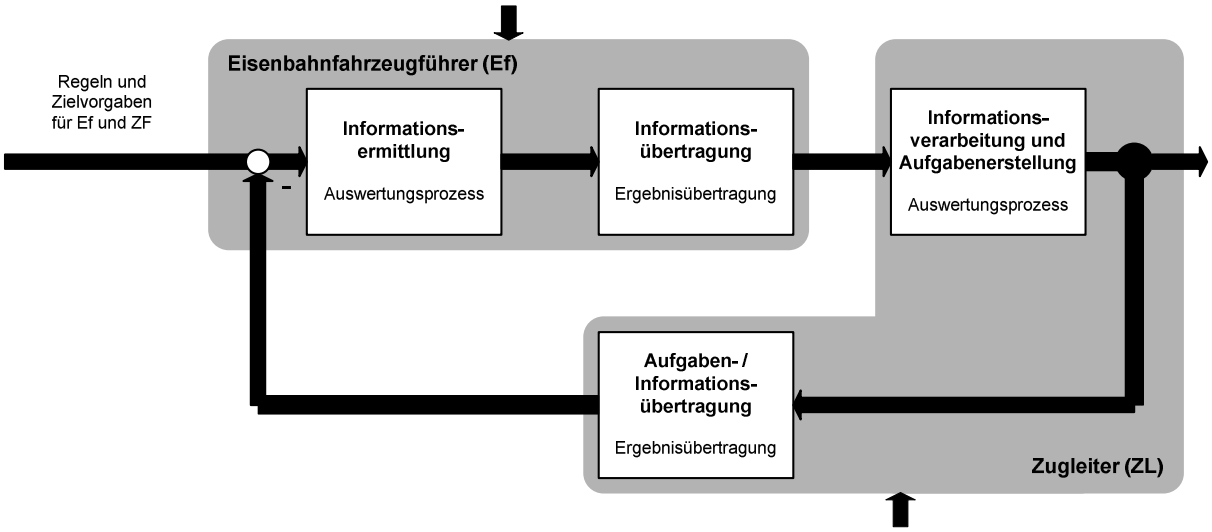

Bild 5.4: Generischer Regelkreis des Betriebsprozesses

Um das Systemmodell der Systemdefinition in den Betriebsprozess zu integrieren, werden die Modelle der funktionalen Systemarchitektur mit dem Prozessmodell verknüpft. Als Basis dient hierbei der PROFUND-Ansatz nach [Slovak 2007], bei dem sicherheitsrelevante Systeme mit Hilfe von Petrinetzen strukturiert analysiert werden können. PROFUND steht dabei für die Modellierung des Systemprozesses (PRO) der funktionalen Struktur des sicherheitsrelevanten Systemteils (FUN) sowie der Verlässlichkeitsstruktur der jeweiligen Komponente (D = Dependability). Die Verlässlichkeit wird in der hier dargestellten Methode in den Modellen vernachlässigt.

5.2.1.3 Gefährdungsanalyse

Das zu untersuchende System wird in Verbindung mit einem Betriebsprozess in der Analysefolge als ein zusammenhängendes System betrachtet.

Das System gilt als „sicher“, wenn von ihm keine Gefährdungen ausgehen. Umgangssprachlich wird häufig der Begriff „Gefährdung“ oder auch „Gefährdungsidentifikation“ synonym verwendet, da der Mensch – in der Regel „Ich-bezogen“ – die auf ihn einwirkenden Gefährdungen und nicht die systembezogenen Gefährdungen analysieren möchte. Weiterführende Betrachtungen sind in [Drewes/May 2007] sowie zur Definition in [Schnieder 2009] zu finden.

Um die Begrifflichkeit der „Gefährdung“ noch zu verdeutlichen, stellt Bild 5.5 in Form eines Petrinetzes die kausale Abhängigkeit mehrerer Ursachen bzw. gefährdender Bedingungen dar, die erst durch den Eintritt eines gefährdenden und unerwünschten Ereignisses zu einem gefährlichen Zustand führen können. Diese Kombination wird letztendlich mit dem Begriff „Gefährdung“ definiert. Jede gefährdende Bedingung hat wiederum diverse Vorbedingungen, die an dieser Stelle nicht tiefer gehend betrachtet werden.

Die aus der Gefährdung resultierenden Konsequenzen können sowohl ein Schaden als auch der sichere Zustand sein, der mittels geeigneter Sicherungsprozesse erreicht werden kann.

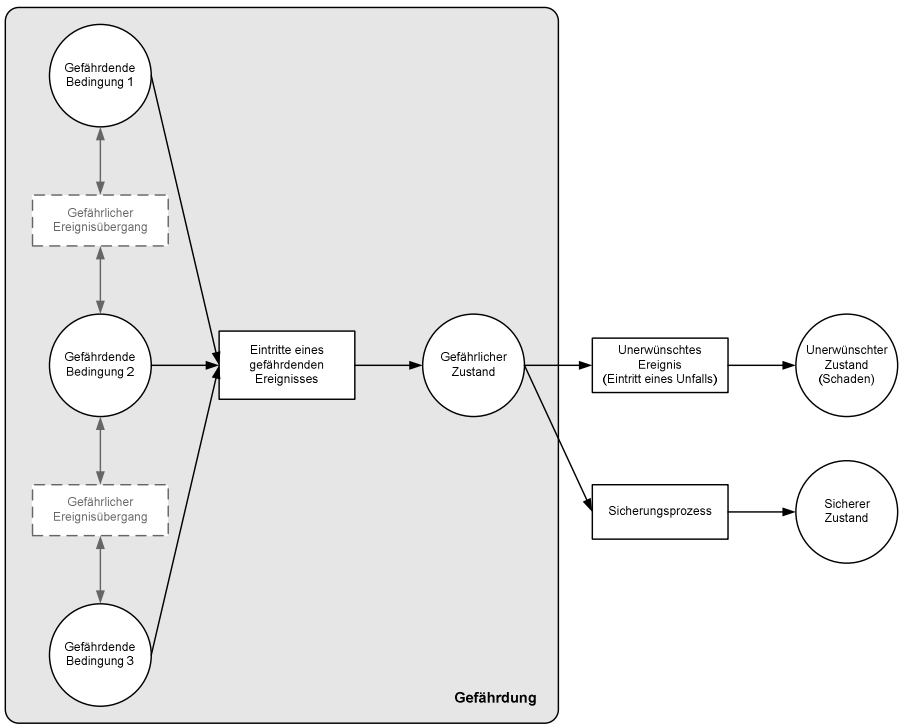

Bild 5.5: Strukturierung von „Gefährdung“

Auf Grundlage der Definition von „Gefährdung“ werden potenzielle Schadens- bzw. Unfallereignisse für die weitere Betrachtung herausgearbeitet. Bild 5.6 stellt die möglichen Unfallarten im Schienenverkehr dar.

Dominierend im Eisenbahnbereich sind Kollisionen und Entgleisungen. Sonstige Unfälle durch z.B. Feuer, Wasser, Elektrizität etc. werden an dieser Stelle nicht weiter betrachtet, da sie durch das Ortungssystem primär nicht hervorgerufen werden können [Drewes/May 2007].

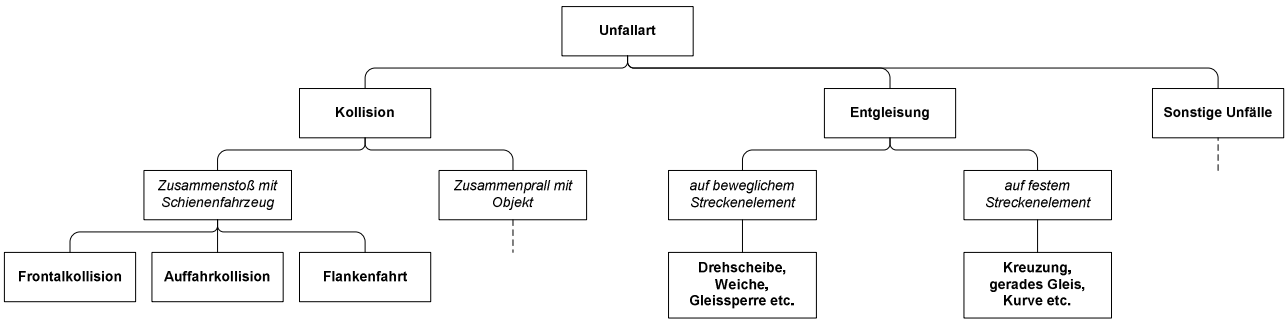

Bild 5.6: Schadensereignisse und Unfallarten im Schienenverkehr

Mit Hilfe der Definition und der Darstellung möglicher Konsequenzen ist es das Ziel der Gefährdungsidentifikation, herauszufiltern, welche Gefährdungen einen unerwünschten Zustand (Schaden) herbeiführen können. Diesen Gefährdungen muss dann entsprechend durch risikoreduzierende Maßnahmen im Nachhinein begegnet werden, so dass durch geeignete Sicherungsprozesse im Fall einer auftretenden Gefährdung möglichst immer der sichere Zustand erreicht wird (vgl. Bild 5.5).

Sofern möglich, sind für die weitere Bearbeitung Gefährdungslisten heranzuziehen, wodurch mit maximal möglicher Vollständigkeit Systemgefährdungen identifiziert werden können und sich Sicherheitsanforderungen automatisch ableiten lassen [Drewes/May 2007].

5.2.1.4 Ursachen- und Folgenanalyse

Auf Grundlage der Gefährdungsidentifikation werden Gefährdungen und sicherheitsrelevante Anforderungen ermittelt. Als Eingangsinformationen werden diese in die FMEA als methodische Grundlage der Ursachen- und Folgenanalyse eingebracht. Betrachtet wird jeweils eine Funktion eines Teilsystems in einer Baumstrukturanalyse. Der jeweiligen Funktion wird ein potenzieller Fehler zugeordnet und entsprechende Fehlerfolgen und -ursachen abgeleitet und begründet. Tabellarisch werden die Informationen mittels der FME(C)A verarbeitet und anschließend quantitativ abgeschätzt.

5.2.1.5 Risikoabschätzung

Als Erweiterung der FMEA wird durch Abschätzung der Auftretenswahrscheinlichkeit der Fehlerursache, dem Bedeutungsgrad der Fehlerfolge und der Entdeckungswahrscheinlichkeit des Fehlers die Risikoprioritätszahl (RPZ) ermittelt, sodass jetzt von einer FMECA ausgegangen wird. Für die Einstufung der Werte für die RPZ werden die Zuordnungstabellen (Bilder 5.7 und 5.8) herangezogen. Durch die FMECA kann jetzt jeder Funktion ein potenzielles Risiko gegenüber gestellt werden. Als tolerierbarer Grenzwert wird, wie in Abschnitt 4.2.4 beschrieben, die RPZ = 50 angenommen. Die potenziellen Risiken werden im anschließenden Arbeitsprozess über die ermittelten RPZ-Werte analysiert.

5.2.1.6 Risikobewertung

Die abgeschätzten RPZ-Werte der FMECA sind in der Prozessfolge zu bewerten. Aufgrund ähnlicher Strukturen der Risikoabschätzung bei der FMECA und der Einstufung in der Risikomatrix (vgl. Bild 4.7) lässt sich ein Zusammenhang für eine durchgängige Methode herstellen. Die in Bild 4.7 aufgeführten Klassifizierungen bezüglich der Auftretenswahrscheinlichkeit der Fehlerursache bzw. der Häufigkeit von Gefährdungsfällen sind in Anlehnung an die DIN EN 50126 entsprechend der Risikoprioritätszahlbewertung (RPZ) auf zehn Kategorien in dieser Methode (Bilder 5.7 und 5.8) verfeinert worden, wodurch eine genauere qualitative Einstufung der Gefährdung möglich wird.

Auftretenswahrscheinlichkeit der Fehlerursache bzw. Häufigkeit von Gefährdungsfällen	**Definition**
sehr häufig = 10	Wird sehr häufig auftreten. Das Auftreten der Fehlerursache bzw. die Gefahr sind ständig gegenwärtig.
häufig = 9	Wird häufig auftreten. Das Auftreten der Fehlerursache bzw. die Gefahr sind häufig gegenwärtig.
sehr wahrscheinlich = 8	Wird mehrmals auftreten. Es ist zu erwarten, dass die Fehlerursache bzw. Gefahr sehr oft eintritt.
wahrscheinlich = 7	Wird mehrmals auftreten. Es ist zu erwarten, dass die Fehlerursache bzw. Gefahr oft eintritt.
gelegentlich = 6	Kann mehrmals auftreten. Es ist zu erwarten, dass die Fehlerursache bzw. Gefahr mehrmals eintritt.
selten = 5	Kann manchmal während des Lebenszyklus auftreten. Mit dem Eintreten ist zu rechnen.
unwahrscheinlich = 4	Das Auftreten ist unwahrscheinlich, aber möglich. Es darf angenommen werden, dass die Fehlerursache bzw. Gefahr in Ausnahmefällen eintritt.
möglich = 3	Das Auftreten ist sehr unwahrscheinlich, aber möglich. Es darf angenommen werden, dass die Fehlerursache bzw. Gefahr nur in Ausnahmefällen eintritt.
relativ unvorstellbar = 2	Das Auftreten ist relativ unwahrscheinlich. Es darf angenommen werden, dass die Fehlerursache bzw. Gefahr kaum eintritt.
absolut unvorstellbar = 1	Das Auftreten ist extrem unwahrscheinlich. Es darf angenommen werden, dass die Fehlerursache bzw. Gefahr nicht eintritt.

Bild 5.7: Definition Häufigkeit von Gefährdungsfällen, angelehnt an [EN 50126]

Bezüglich der Bedeutung der Fehlerfolge bzw. der Gefährdungsstufen stellt Bild 5.8 die Bedeutungen der einzelnen Klassifizierungen vor. Zur Vergleichbarkeit wurden, in Anlehnung an die DIN EN 50126, die dort enthaltenen vier Kategorien entsprechend der Risikoprioritäts-zahlbewertung (RPZ) – (B) Bedeutung der Fehlerfolge aus Anwendersicht – in zehn Kategorien verfeinert, wodurch ebenfalls eine genauere qualitative Einstufung der Gefährdung ermöglicht wird.

Bedeutung der Fehlerfolge bzw. Gefährdungsstufen	**Konsequenzen für Personen und Umwelt**
katastrophal = 10	Mehrere Unfalltote und zahlreiche Schwerverletzte und schwere Umweltschäden
sehr kritisch = 9	Einzelne Unfalltote und/oder mehrere Schwerverletzte und nennenswerte Umweltschäden
kritisch = 8	Einzelner Unfalltoter und/oder Schwerverletzter und nennenswerte Umweltschäden
kritisch marginal = 7	Schwere Verletzungen und nennenswerte Bedrohung der Umwelt.
marginal kritisch = 6	Leichte Verletzungen und/oder nennenswerte Bedrohung der Umwelt.
marginal = 5	Kleinere Verletzungen und/oder nennenswerte Bedrohung der Umwelt.
leicht marginal = 4	Kleinste Verletzung und/oder kaum nennenswerte Bedrohung der Umwelt.
leicht = 3	Mögliche kleinere Verletzung.
unbedeutend = 2	Mögliche aber geringfügige Verletzung.
absolut unbedeutend = 1	Kaum Verletzungen denkbar.

Bild 5.8: Definition Konsequenzen und Gefährdungsstufen, angelehnt an [EN 50126]

Die Entdeckungswahrscheinlichkeit des Fehlers gilt bei der Risikobewertung als erster reduzierender Faktor, der bereits in der RPZ berücksichtigt ist und ebenso tabellarisch zwischen „Entdeckungswahrscheinlichkeit ist hoch = 1“ und „Entdeckungswahrscheinlichkeit ist gering = 10“ eingestuft wird. Ergänzende Betrachtungen zu geeigneten Risikoreduktionen sind entsprechend im Nachgang zu berücksichtigen. Die dann ermittelten Risiken sind bei der weiteren Untersuchung genauer zu bewerten und mit Hilfe von Risikoakzeptanzkriterien, z.B. dem Nachweis der mindestens gleichen Sicherheit mit einem Referenzsystem, einzustufen.

Wird nun in Abhängigkeit der RPZ-Faktoren und dem Grenzwert von 50 eine neue RPZ-Risikomatrix aufgestellt, ergibt sich eine 10x10-Matrix, die um den Faktor der Entdeckungswahrscheinlichkeit dreidimensional erweitert werden könnte. Bild 5.9 stellt die entwickelte RPZ-Risikomatrix für den schlechtesten Fall dar, dass die Entdeckungs-wahrscheinlichkeit 10 (gering) beträgt und somit im ersten Ansatz keine primäre Risikoreduktion besteht.

Bei dieser Einstufung wird deutlich, dass es einen unteren Bereich (hell bzw. grün markiert) gibt, bei dem die Entdeckungswahrscheinlichkeit unberücksichtigt bleiben kann und trotzdem sämtliche Risikobetrachtungen im sicheren bzw. restrisikobehafteten Bereich (RPZ < 50) liegen.

	Risikomatrix mit RPZ										
	Auftretenswahrscheinlichkeit der Fehlerursache										
10	sehr häufig										
9	häufig										
8	sehr wahrscheinlich										
7	wahrscheinlich										
6	gelegentlich										
5	selten										
4	unwahrscheinlich										
3	möglich										
2	relativ unvorstellbar										
1	absolut unvorstellbar										
		absolut unbedeutend	unbedeutend	leicht	leicht marginal	marginal	marginal kritisch	kritisch marginal	kritisch	sehr kritisch	katastrophal
		1	2	3	4	5	6	7	8	9	10
		Bedeutung der Fehlerfolge aus Anwendersicht									
	Risikomatrix bei Entdeckungswahrscheinlichkeit = 10										

Bild 5.9: RPZ-Risikomatrix mit Entdeckungswahrscheinlichkeit = 10 (gering)

Zum Vergleich verdeutlicht Bild 5.10 die Verlagerung der Bewertung bei einer sehr hohen Entdeckungswahrscheinlichkeit von 1 (hoch). Aufgrund der potenziellen Risikoreduktion durch die Entdeckung des Fehlers liegt der große untere Teil (hell bzw. grün markiert) im sicheren, restrisikobehafteten Bereich (RPZ < 50). Auf Grundlage der getroffenen Annahmen können Bewertungsergebnisse in diesem Bereich ohne weitere Betrachtung als restrisikobehaftet und somit sicher angenommen werden.

Im Gegensatz dazu muss jedem Wert im dunklen bzw. roten Bereich durch anderweitige risikoreduzierende Maßnahmen begegnet werden, da dort auch eine sofortige Entdeckung eines Fehlers keinen sicheren Zustand mehr gewährleisten kann.

	Risikomatrix mit RPZ										
	Auftretenswahrscheinlichkeit der Fehlerursache										
10	sehr häufig										
9	häufig										
8	sehr wahrscheinlich										
7	wahrscheinlich										
6	gelegentlich										
5	selten										
4	unwahrscheinlich										
3	möglich										
2	relativ unvorstellbar										
1	absolut unvorstellbar										
		absolut unbedeutend	unbedeutend	leicht	leicht marginal	marginal	marginal kritisch	kritisch marginal	kritisch	sehr kritisch	katastrophal
		1	2	3	4	5	6	7	8	9	10
		Bedeutung der Fehlerfolge aus Anwendersicht									
	Risikomatrix bei Entdeckungswahrscheinlichkeit = 1										

Bild 5.10: RPZ-Risikomatrix mit Entdeckungswahrscheinlichkeit = 1 (hoch)

Durch den Vergleich der beiden RPZ-Risikomatrizen (Bilder 5.9 und 5.10) lässt sich eine Schnittmenge ermitteln in der die Werte für die Entdeckungswahrscheinlichkeit zwischen 2 und 9 liegen. RPZ-Ergebnisse, die sich in diesem Bereich befinden sind durch geeignete

risikoreduzierende Maßnahmen zu bewerten. In Bild 5.11 sind die Bereiche „sicher“ und „nicht sicher“ sowie das Streuband der risikoreduzierenden Entdeckungswahrscheinlichkeit zusammenfassend gegenüber gestellt. Durch das Streuband wird gleichzeitig eine Schadenskurve symbolisiert, die ggf. volkswirtschaftlich bewertet werden könnte, wodurch weitere innovative Betrachtungen abgeleitet werden könnten.

Ebenfalls im Streuband dargestellt sind exemplarisch die Kurven der RPZ = 50 sowie der RPZ = 125 (vgl. Abschnitt 4.2.4). RPZ-Werte oberhalb des Grenzrisikos von 50, insbesondere aber auch oberhalb der Grenze von 125 sind durch geeignete Maßnahmen risikoreduzierend durch folgende Möglichkeiten zu betrachten:

1. Schutzmaßnahmen – Systemoptimierung zur Reduktion der Fehlerfolge (*B*)
2. Diagnose- oder Redundanzmaßnahmen – Gefahrenabwehr durch Erhöhung der Entdeckungswahrscheinlichkeit (*E*)
3. Häufigkeit reduzieren – Gefährdungsreduktion durch Systemqualität im V-Prozess (*A*)

Dies wird in Bild 5.11 durch die anschauliche Gegenüberstellung der Potenziale der Risiko-reduktion dargestellt.

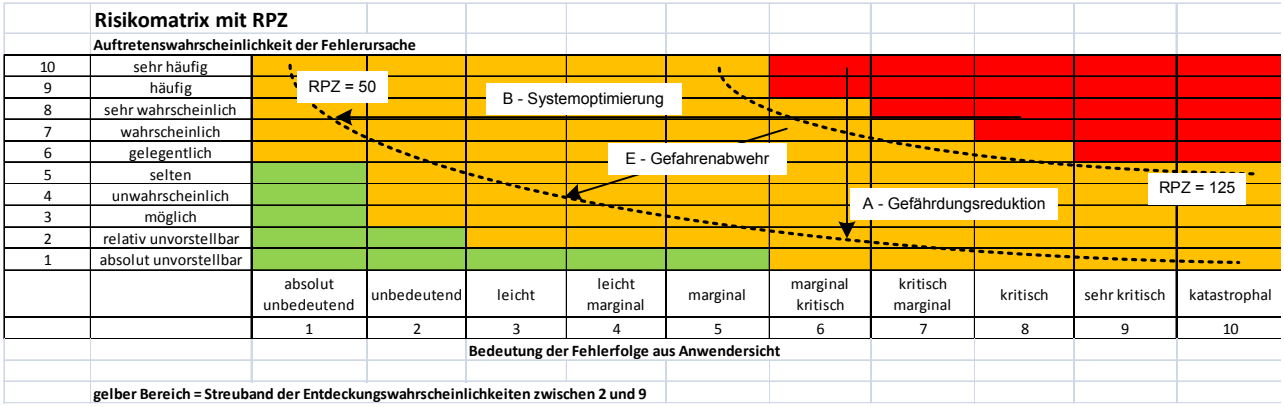

Bild 5.11: RPZ-Risikomatrix mit Streuband der Entdeckungswahrscheinlichkeit

Zur abschließenden Bewertung werden die Ergebnisse der FMECA-Betrachtungen in eine Risikoskala eingefügt (Bild 5.12). Das Grenzrisiko zwischen vernachlässigbarer und zu tolerierender Risikokategorie (RPZ = 50) muss der Einordnung in der RPZ-Risikomatrix entsprechen. Durch dieses methodische Vorgehen werden erforderliche Risikoreduktionen im Folgeprozess anschaulich verdeutlich.

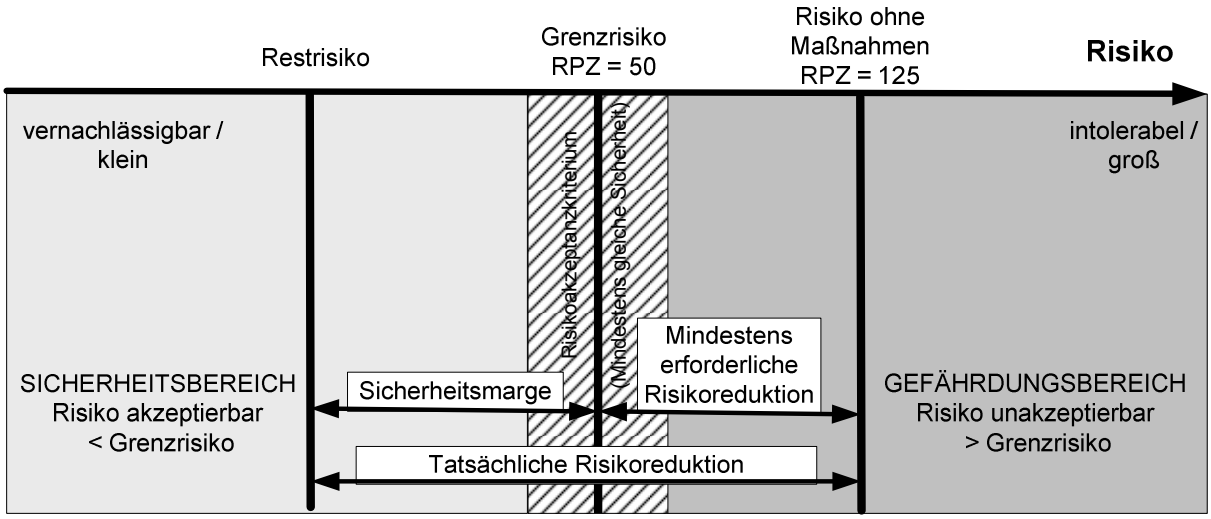

Bild 5.12: Nominale, quantitative Risikoskala nach [Slovak 2007]

Durch die Gegenüberstellung der Risikomatrix, des Sicherheits- und Verfügbarkeitsdiagramms und der RPZ als semiquantitativer Anteil wird deutlich, dass ein mathematischer Zusammenhang zwischen der Auftretens- und der Entdeckungswahrscheinlichkeit besteht. Die Entdeckungswahrscheinlichkeit wird bei der Berechnung bereits als risikoreduzierende Größe berücksichtigt und reduziert somit die Auftretenswahrscheinlichkeit.

Die Größen *A* und *E* der RPZ könnten somit auch zusammengefasst werden, wodurch die Aussagekraft der zweidimensionalen Risikomatrix weiterhin erhalten bliebe und eine Reduzierung der FMECA auf zwei Werte zu überdenken wäre.

5.2.1.7 Beherrschung der Systemgefährdungen

Mit Einführung der CENELEC-Normen wurde der Sicherheitsbegriff neu geprägt und mit „Freiheit von unvertretbaren Risiken“ umschrieben. Die Basis bildet der Gedanke, dass gesellschaftlich ein gewisses Restrisiko akzeptiert werden muss, da komplexe technische Systeme nicht absolut fehler- und/oder ausfallfrei umgesetzt werden können. Dieses Restrisiko wird über das bereits erläuterte tolerierbare Grenzrisiko (RPZ = 50) definiert und muss durch die Betrachtung des Herstellers unter Berücksichtigung und Realisierung aller wirksamen Schutzmaßnahmen unterschritten werden (Bild 5.12).

Bei der funktionalen Betrachtung komplexer Systeme bezüglich der Sicherheit ist stets zu berücksichtigen, dass bei der Eisenbahn die Sicherheit der Betriebsführung an oberster Stelle steht [AEG 2008]. Als grundlegende Vorgabe sind daher sämtliche Betriebsabläufe aus sicherheitsrelevanten Gründen in exakt strukturierten kausalen Handlungsfolgen organisiert; die einzelnen Prozessschritte müssen logisch aufeinander folgend aufgebaut sein. Eine Systemgefährdung muss dabei zu einer Prozessunterbrechung führen, wobei stets von einem aktiven Informationsfluss ausgegangen wird. Beim Ausbleiben einer positiven Information muss eine Hemmung eintreten. Fehlerausschluss, -abwehr und -offenbarung sind dabei als Ziele der zu treffenden Maßnahmen zu

berücksichtigen [Drewes 2009]. In einer Sicherheitsuntersuchung ist diesen Vorgaben entsprechend zu begegnen und deren Umsetzung und Erfüllung zu belegen. Tiefer gehende Untersuchungen zur Risikobetrachtung als Teil der Sicherheitsuntersuchung bei Bahnsystemen finden sich in [Slovak 2007] und [Braband 2005].

5.2.2 Abgrenzung zwischen Sicherheitsanalyse und -nachweis

Während sich die Sicherheitsanalyse mit den Vorbetrachtungen der Sicherheit eines Systems beschäftigt, in dem Annahmen darüber getroffen werden, wie sicher ein System auf Basis des Standes der Technik sein soll (vgl. Bild 4.4), werden im Rahmen des Sicherheitsnachweises die getroffenen Annahmen bzw. Spezifikationen nachgewiesen und für eine spätere Systemzulassung festgelegt. Für das betrachtete System werden die Spezifikationen in der Phase der Systemdefinition fixiert.

Normative Inhalte und Realisierungsbestimmungen sind Bestandteile zur Berücksichtigung bei der Sicherheitsnachweisführung. Während der Sicherheitsanalyse wird auf Grundlage der DIN EN 50126 entsprechend der ersten Lebenszyklusphasen nach dem V-Modell gearbeitet. Der Sicherheitsnachweis stützt sich auf die DIN EN 50129; er wird begleitend und auch zu den späteren Lebenszyklusphasen der Entwicklung erstellt. Die vorgenannte Abgrenzung wird in Bild 5.13 verdeutlicht, in dem für ein generisches und sicherheitsrelevantes Produkt die Lebenszyklusphasen bis zur Systemzulassung nach DIN EN 50126 dargestellt sind. Auf der rechten Bildseite ist die Zuordnung des Sicherheitsnachweises hervorgehoben.

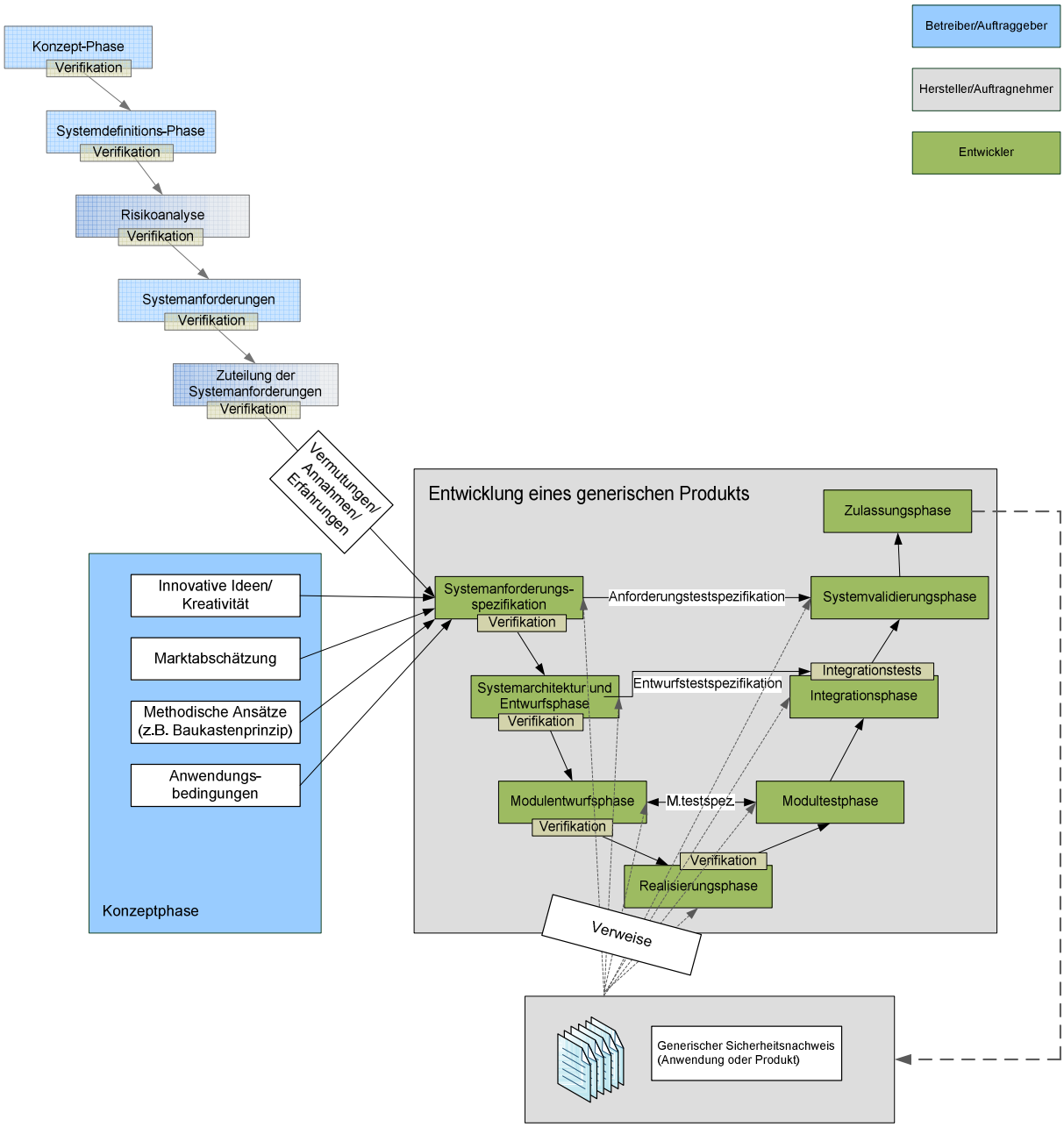

Bild 5.13: V-Modell einer generischen Produktentwicklung mit Sicherheitsnachweis

Fortlaufende Ergebnisse der Sicherheitsanalyse aus den phasenbezogenen Sicherheitsaktivitäten werden in einem Sicherheitsbericht festgehalten, der als Eingangsdokument dem Sicherheitsnachweis zur Verfügung gestellt wird.

5.2.3 Sicherheitsnachweis

Ein Sicherheitsnachweis als Bestandteil der Sicherheitsuntersuchung ist ein dokumentierter Nachweis, dass ein Produkt die spezifizierten Sicherheitsanforderungen erfüllt. Begleitend zu Untersuchung des Systems unter Berücksichtigung sicherheitsrelevanter Aspekte ist entsprechend parallel ein Sicherheitsnachweis nach DIN EN 50129 zu führen. Neben den Nachweisen des

Qualitäts- und Sicherheitsmanagements der Hersteller sind die funktionale sowie die technische Sicherheit des Systems nachzuweisen. Der Sicherheitsnachweis selbst gliedert sich nach der [EN 50129] in sechs relevante Teile (Bild 5.14), welche jeweils als gesonderte Dokumente zu erstellen sind; geeignete Verweise auf andere Dokumente reichen jedoch bei der Erstellung des Nachweises meist aus. Der technische Sicherheitsbericht (Teil 4, vgl. Bild 5.14), welcher auch für nicht sicherheitsrelevante Anwendungen herangezogen werden kann, gliedert sich in sechs weitere Unterabschnitte, die der Erleichterung der vollständigen Abarbeitung dienen.

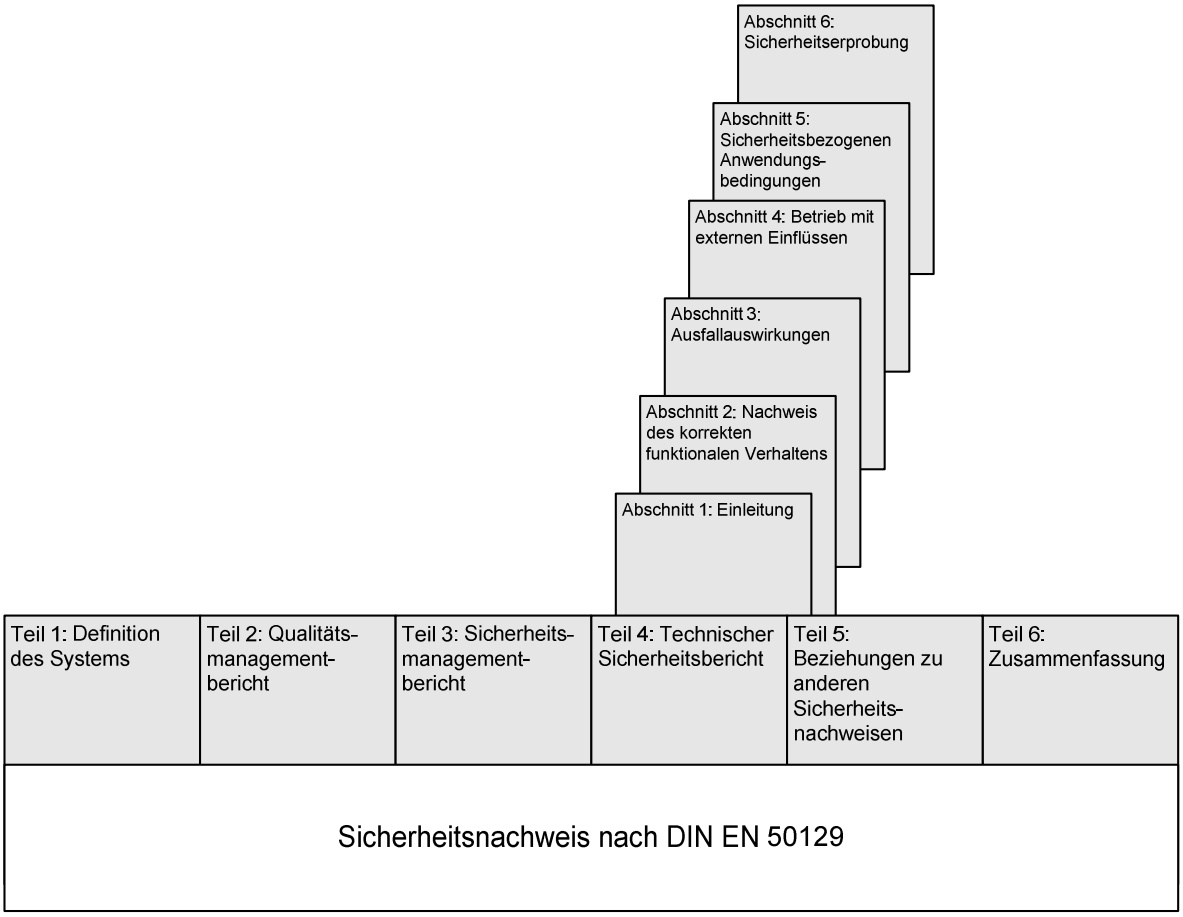

Bild 5.14: Struktur des Sicherheitsnachweises nach [EN 50129]

Weitere Bestandteile der Sicherheitsdokumentation sind die Verantwortungsstrukturen der Sicherheitsorganisation im entwickelnden Unternehmen, die Erstellung eines Sicherheitsplans etc. Nach erfolgter Entwicklung und begleitender Dokumentation kann das sicherheitsrelevante System einem Sicherheitszulassungsverfahren unterzogen werden. Im Vorfeld dazu muss der Sicherheitsnachweis von einer unabhängigen Einrichtung begutachtet werden, um zu gewährleisten, dass die erforderliche und spezifizierte Sicherheitsanforderungsstufe (SIL) erreicht wurde. Dieses wird mit der Erstellung eines Sicherheitsgutachtens belegt.

Für ein generisches Produkt sind die System- und Sicherheitsanforderungsspezifikationen, der Sicherheitsnachweis und das unabhängige Sicherheitsgutachten der Aufsichtsbehörde einzureichen, um eine Systemzulassung zu erhalten.

Änderungen nach der Systemzulassung haben zur Folge, dass diese unter Berücksichtigung des Qualitäts- und Sicherheitsmanagements umzusetzen sind, und die begleitende Dokumentation so zu erfolgen hat, als würde ein neues System entwickelt werden. Verweise auf bestehende Dokumentationen reichen dabei aus. Nach erfolgten Änderungen ist auch eine erneute Zulassung des Systems erforderlich.

5.2.3.1 Methode der Sicherheitsnachweisführung

Nachfolgend wird das grundsätzliche methodische Vorgehen mit den mindestens erforderlichen Inhalten zur Sicherheitsnachweisführung erläutert, ein exemplarischer, dokumentierter Nachweis wird im Folgenden nicht vorgestellt, da in dieser Arbeit die Methode im Vordergrund steht.

Im Fall des sicherheitsrelevanten Ortungssystems ist ein spezifischer Sicherheitsnachweis für das System als „generisches“ Produkt zur Anwendung in Sicherungssystemen entsprechend der Struktur in Bild 5.14 zu erstellen. Das Ortungssystem selbst muss dabei den Lebenszyklusprozess entsprechend dem V-Modell nach DIN EN 50126 durchlaufen; mit dem übergeordneten Sicherungssystem muss entsprechend verfahren werden. In der Entwicklungsphase des übergeordneten Systems sind die Dokumentationen und insbesondere der Sicherheitsnachweis des Ortungssystems zu berücksichtigen und entsprechend in das Gesamtsystem zu integrieren.

Bild 5.15 stellt den Zusammenhang des Sicherheitsnachweises als Dokumentation mit Verweismöglichkeiten her.

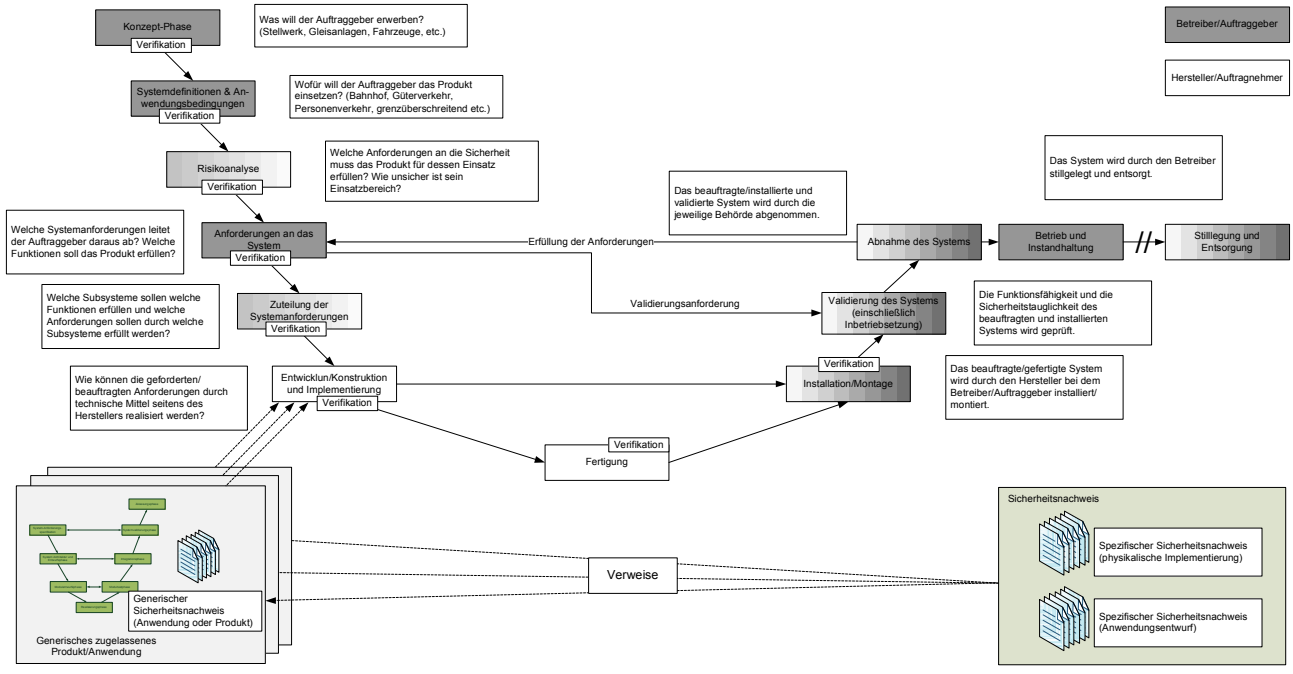

Bild 5.15: V-Modell im Zusammenhang mit Sicherheitsnachweis

Im Rahmen der Sicherheitsuntersuchung wird der Sicherheitsnachweis rein dokumentarisch und in Ergänzung zur Sicherheitsanalyse durchgeführt.

Der dokumentarische Aufwand scheint dabei im ersten Moment erheblich. Bei der Entwicklung und Realisierung eines sicherheitsrelevanten Produktes ist mit dieser Vorgehensweise aber berücksichtigt, dass systematisch eingearbeitete Fehler vermieden und zufälligen Fehlern geeignet begegnet werden kann. Doppelentwicklungen sowie überdimensionierte Redundanzen können somit vermieden werden, was nicht zuletzt Kosten senkt und den Mehraufwand gerechtfertigt.

In den folgenden Unterabschnitten wird das grundsätzliche methodische Vorgehen mit den mindestens erforderlichen Inhalten zur Sicherheitsnachweisführung entsprechend den Grundlagen aus Bild 5.14 vorgestellt.

5.2.3.2 Qualitätsmanagementbericht

Für eine sicherheitsrelevante Produktentwicklung unter Berücksichtigung der DIN EN 50129 muss die Qualität des zu entwickelnden Systems durch ein herstellerseitiges Qualitätsmanagementsystem nach [ISO 900x] gewährleistet werden. Über den gesamten Lebenszyklus des Systems muss dieses anwendbar sein und durch die verantwortlichen Bearbeiter angewendet werden können. Der Einfluss des Qualitätsmanagements auf die Produktentwicklung muss in einem Qualitätsmanagementbericht dargelegt werden. Bestehen bereits eingeführte Qualitätsmanagementprozesse, welche in gleicher Weise mehrfach Anwendung finden, kann auf die entsprechenden Dokumentationen verwiesen werden.

Folgende Aspekte sollten im Qualitätsmanagementbericht für das sicherheitsrelevante System betrachtet und berücksichtigt werden:

- Aufbau der Organisationsstruktur des entwickelnden Unternehmens
- Durchführung der Qualitätsplanung und Aufstellung von Qualitätsverfahren für das System
- Vollständige Spezifikation von Systemanforderungen inkl. Plausibilisierung
- Kontrolle der Entwurfsplanung
- Verifikation des Entwurfs und externe Begutachtung
- Durchführung eines anwendungsorientierten Engineerings
- Qualitätsorientierte Beschaffung von Komponenten sowie Herstellung
- Eindeutige Produktidentifikation und Verfolgbarkeit aller Prozessschritte
- Qualitätsorientierte Handhabung und Lagerung von Dokumenten und Teilprodukten
- Kontinuierliche Überprüfungen und Tests (Verifikationen)
- Festlegung von Korrekturmaßnahmen bei Abweichungen
- Festlegung von Verpackung und Form der Lieferung
- Qualitätsorientierte Installation und Inbetriebnahme beim Kunden

- Durchführung des Betriebes und Instandhaltung des Systems nach Qualitätsgesichtspunkten
- Qualitätsüberwachung und Rückkopplung nach jedem Prozessschritt
- Erstellung und Archivierung von Dokumentationen und Aufzeichnungen aller Art
- Konfigurationsmanagement und Steuerung von Änderungen
- Aufzeichnung der jeweiligen Bearbeiterkompetenz und dem zugehörigen Ausbildungsstand
- Festlegung von Qualitätsaudits und fortlaufender Qualitätsverfolgung
- Festlegung von systemgerechter Stilllegung und umweltgerechter Entsorgung des Systems

Für alle Sicherheitsanforderungsstufen (SIL) sind Begutachtungen des Sicherheitsplans nach evtl. Änderung sowie nach jeder Phase des Sicherheitslebenszyklus sehr empfohlen (highly recommended) [EN 50129]. Den Bearbeitern wird die Erstellung von Checklisten über ihre Tätigkeiten für alle Sicherheitsanforderungsstufen nahegelegt. Die „sehr empfohlenen“ und somit relevanten Dokumentationen in der Entwurfsphase erstrecken sich auf die:

- graphische Beschreibung von Teilsystemen
- Beschreibungen der Schnittstellen
- Festlegung von Änderungsprozeduren
- Aufstellung eines Instandhaltungshandbuches
- begleitende Herstellungsdokumentation
- systemzugehörige Dokumentation für den Systembetreiber bzw. Nutzer

Zusätzlich werden Umgebungsstudien bezüglich der elektromagnetischen Verträglichkeit (EMV) [EN 50121], der Vibration usw. im Rahmen des Qualitätsmanagementberichtes empfohlen [EN 50129].

5.2.3.3 Sicherheitsmanagementbericht

Inhalt des Managementberichts ist die Nachweisführung, dass für den gesamten Sicherheitslebenszyklus des betrachteten Systems ein Sicherheitsmanagementprozess besteht und stetig umgesetzt wird. Die Sicherheit des Systems muss auf der Stufe der Realisierung durch ein entsprechendes Sicherheitsmanagementsystem gewährleistet werden. Eine klare Trennung zwischen Entwicklungs- und Prüftätigkeiten ist darin zu berücksichtigen.

Informationen aus nachfolgenden Bereichen müssen im Sicherheitsmanagementbericht enthalten sein:

1. Die herstellerbezogene Sicherheitsorganisation mit Verantwortlichkeiten, Kompetenzen und der Festlegung von Unabhängigkeiten entsprechend der systembezogenen Sicherheitsanforderungsstufe.

Detaillierung: Der Sicherheitslebenszyklus muss in einer geeigneten Sicherheitsorganisation ablaufen, die vorrangig aus qualifiziertem Personal mit einer klaren Rollenverteilung besteht. Qualifikation der Mitarbeiter für die jeweilige Aufgabe (Ausbildung, Erfahrung, Wissen etc.), ihre Rolle und die Durchführung von Schulungen in sicherheitsrelevanten Tätigkeiten müssen im Sicherheitsmanagementbericht dokumentiert werden.

Dabei müssen die Mitarbeiter für Tätigkeiten in den Sicherheitsanforderungsstufen SIL 1 und SIL 2 mindestens über eine technische Ausbildung bzw. ausreichend Erfahrungen, für SIL 3 und SIL 4 über eine höhere technische Ausbildung bzw. eine weitreichende Erfahrung verfügen. Eine Schulung oder Einweisung der Mitarbeiter ist am Anfang aller sicherheitsrelevanten Aufgaben erforderlich, welche je nach SIL-Level auch mehrfach durchgeführt werden muss.

Die Rollen des Entwicklers und des Verifizierers bzw. Validierers sind klar zu trennen und dokumentativ zu erfassen. Die Begutachtung erfolgt durch geeignete Mitarbeiter einer unabhängigen Organisation.

2. Die Sicherheitsplanung inkl. aller sicherheitsrelevanten Tätigkeiten und Projektmeilensteine bezogen auf die Sicherheit.

   In einem Sicherheitsplan müssen die Sicherheitsmanagementstruktur, sicherheitsrelevante Tätigkeiten und Zulassungsmeilensteine während des Systemlebenszyklus enthalten sein, wobei auch Hard- und Software zu betrachten sind. Im Hinblick auf Software ist die DIN EN 50128 heranzuziehen [EN 50128].

   Der Sicherheitsplan ist in festzulegenden Zeitabständen zu überprüfen. Ergänzend muss der Sicherheitsplan nach Änderungen oder Ergänzungen des Systems überprüft und ggf. überarbeitet werden, die Auswirkungen der Änderungen auf die Sicherheit müssen dabei bewertet werden.

3. Ein Gefährdungslogbuch inkl. Liste aller Gefährdungen und deren Risikobeherrschung aus der Sicherheitsanalyse mit dem Prozess zur Aktualisierung der Risikoanalyse (soweit erforderlich).

   Sämtliche Gefährdungen, die von dem System ausgehen oder potenziell auf das System einwirken können und während des Systemlebenszyklus erkannt werden, müssen in einem Gefährdungslogbuch geeignet vermerkt werden. Ergänzende Informationen sollten mit dem Datum der Gefährdungsentdeckung, den Inhalten der Gefährdungsliste inkl. Gefährdungsbeschreibung, den potenziellen Auswirkungen und der Eintrittswahrscheinlichkeit sowie den getroffenen Abhilfemaßnahmen in die Dokumentation aufgenommen werden. Jede neu erkannte Gefährdung, insbesondere auch nach Systemänderungen, führt zu einer Aktualisierung des Logbuches.

4. Die Dokumentation der Sicherheitsanforderungsspezifikation inkl. Sicherheitsfunktion und -integrität für alle Teilsysteme.

Sicherheitsrelevante Anforderungen an das System müssen im Dokument der Sicherheitsanforderungsspezifikation aufgeführt werden. Dieses kann auch Teil der Systemanforderungsspezifikation sein. Die Sicherheitsanforderungen sind im Rahmen der Risikoanalyse nach DIN EN 50126 durch die Betrachtung der tolerierbaren Gefährdungsraten zu ermitteln. Dem System oder auch Teilsystemen müssen in der Dokumentation Sicherheitsanforderungsstufen (SIL) zugewiesen werden.

5. Der Entwurf und die Entwicklung von Systemteilen bezogen auf die Sicherheitsanforderungen.

   Der Systementwurf muss unter Anwendung einer strukturierten „top-down"-Entwurfsmethode erfolgen, wobei parallel eine Dokumentation zu erstellen ist, die anschließend unabhängig begutachtet wird. Der Entwurf muss hierarchisch bis zur Anforderungsspezifikation herunter gebrochen werden; Referenzen zwischen Spezifikations-, Entwurfs-, Stromlaufplan- und Anwenderdokumentation sind dabei zu berücksichtigen.

   Eine eigenständige Modularisierung mit begrenzter Modulgröße wird für den Systementwurf empfohlen, um die Komplexität einfacher zu gestalten. Je höher die Sicherheitsanforderungsstufe gefordert ist, desto modularisierter sollte der Entwurf gestaltet sein [EN 50129].

6. Kontinuierlich müssen Sicherheitsbegutachtungen, welche im Sicherheitsplan spezifiziert sind, durchgeführt und dokumentiert werden.

   Im Sicherheitsplan sind Begutachtungen (Sicherheitsreviews, z.B. von Entwicklungsdokumenten) einzuplanen. Bei Änderungen des Systems müssen die betreffenden Dokumente erneut eine Sicherheitsbegutachtung durchlaufen.

7. Die Darstellung der Sicherheitsverifikation und -validierung inkl. der Unabhängigkeiten der Bearbeiter entsprechend der systembezogenen Sicherheitsanforderungsstufe.

   Die Verifikation zur Prüfung von Sicherheitsanforderungen am Ende der jeweils vorhergehenden Phase sowie die Validierung zur Prüfung der Sicherheitsanforderungsspezifikation auf Systemebene muss ebenfalls bereits im Vorfeld im Sicherheitsplan festgehalten werden. Die Durchführung der Verifikations- und Validierungstätigkeiten ist zu dokumentieren. Bei Änderungen oder Ergänzungen des Systems müssen Verifikation und Validierung auf Basis des neuen Systems wiederholt werden.

   Entwickler, Validierer und Verifizierer müssen je nach Sicherheitsanforderungsstufe (SIL 0 bis 4) einen gewissen Grad der Unabhängigkeit aufweisen. Der Gutachter muss stets unabhängig in Person und Unternehmen sein. Bei SIL 0 ist der Gutachter nur erforderlich, wenn die Sicherheit des Gesamtsystems beeinflusst wird. Bild 5.16 gibt einen Überblick über die geforderten Unabhängigkeiten der Bearbeiter sowie im unteren

Teil über die erforderlichen Maßnahmen und anzuwendenden Methoden während der Verifikations- und Validierungsphase.

Nachgelagerte Planungspunkte im Sicherheitsmanagementbericht:

8. Die Planung der Systemübergabe an den Betreiber mit den Vorbedingungen der Sicherheitsanerkennung sowie der hoheitlichen Sicherheitszulassung.

   Vor der Übergabe des sicherheitsrelevanten Systems an den Eisenbahnbetreiber (Kunden) zum Betriebseinsatz müssen alle legislativen Vorgaben erfüllt sein und das System durch eine Aufsichtsbehörde – in Deutschland i.d.R. das EBA – abgenommen werden. Die Sicherheitsanerkennung und Zulassung erfolgt durch die Aufsichtsbehörde unter Berücksichtigung des Sicherheitsnachweises und des unabhängigen Gutachtens eines der Behörde zuarbeitenden unabhängigen Sachverständigen.

9. Für den Betrieb und die Instandhaltung müssen die im Sicherheitsplan festgelegten Verfahren und Sicherheitsüberwachungen plausibilisiert werden.

   Für den späteren Betriebseinsatz sind Verfahren und Überwachungsprozesse festzulegen, die dem Betreiber in Form von Dokumenten und Schulungen mitgeteilt werden. Diese Inhalte sind zu planen und stets auf Aktualität zu überprüfen.

10. Die Stilllegung und die Entsorgung müssen entsprechend Sicherheitsplan festgelegt sein und plausibilisiert werden.

    Aus Beweggründen des Umweltschutzes sind bereits bei der Systemplanung die Außerbetriebsetzung und die fachgerechte Entsorgung des Systems zu berücksichtigen. Auch diese Inhalte sind zu planen und stets auf Aktualität zu prüfen.

5.2.3.4 Technischer Sicherheitsbericht

Im technischen Sicherheitsbericht ist der Nachweis der ausreichenden technischen und betrieblichen Sicherheit des Systems auf der Stufe des Anwendungsentwurfs zu erbringen. Ebenso ist nachzuweisen, dass Teilsysteme oder Komponenten die Sicherheitsanforderungen im konkreten Anwendungsfall erfüllen und dass deren Einsatzbedingungen eingehalten werden können (Bild 5.16).

	Entwickler / Entwerfer	Verifizierer	Validierer
SIL 0	Kann dieselbe Person sein		
SIL 1 / SIL 2	Gesonderte Bearbeitung	Kann dieselbe Person sein	
SIL 3 / SIL 4	Gesonderte Bearbeitung	Gesonderte Bearbeitung	Gesonderte Bearbeitung
SIL 1	**SIL 2**	**SIL 3**	**SIL 4**
Vorbereitete Checklisten, Konzentration auf Hauptsicherheitsbelange		Vorbereitete, detaillierte Checklisten	
	Simulation		
Funktionale Tests, Reviews sollten durchgeführt werden, die zeigen, dass die spezifizierten Eigenschaften und Sicherheitsanforderungen erfüllt wurden.		Umfassende funktionale Tests sollten auf der Basis wohl definierter Testfälle durchgeführt werden, die zeigen, dass die spezifizierten Eigenschaften und Sicherheitsanforderungen erfüllt wurden.	
Das Testen der sicherheitsrelevanten Funktionen sollte unter den spezifizierten Umgebungsbedingungen durchgeführt werden.		Das Testen der sicherheitsrelevanten Funktionen und anderes Testen sollte unter den spezifizierten Umgebungsbedingungen durchgeführt werden.	
Stoßspannungsfestigkeit sollte an den Grenzwerten der realen Betriebsbedingungen getestet werden.	Stoßspannungsfestigkeit sollte an höheren Grenzwerten der realen Betriebsbedingungen getestet werden.		
Berechnung der Ausfallraten auf Basis der typischen Bedingungen.		Berechnung der Ausfallraten auf Basis von Worst-case-Bedingungen.	
Inspektion aller Dokumentationen			
		Spezifikation von Produktionsanforderungen und Vorsichtsmaßnahmen sowie Audit des tatsächlichen Herstellungsprozesses durch die Sicherheitsorganisation.	
Entwickler von Testhilfsmitteln sollten unabhängig von System- oder Produktentwicklern sein		Entwickler von Testhilfsmitteln sollten unabhängig von System- oder Produktentwicklern sein.	
An geeigneten Stellen im Lebenszyklus sollten Reviews durchgeführt werden, die zeigen, dass die spezifizierten Eigenschaften und Sicherheitsanforderungen erfüllt wurden.			
Spezifikation von Installations- und Instandhaltungsanforderungen und Vorsichtsmaßnahmen.		Spezifikation von Installations- und Instandhaltungsanforderungen und Vorsichtsmaßnahmen sowie Audit der tatsächlichen Installations- und Instandhaltungsprozesse durch die Sicherheitsorganisation.	
Hohes Vertrauen durch Betriebsbewährung von 10.000 Betriebsstunden über mindestens ein Jahr.		Hohes Vertrauen durch Betriebsbewährung von 1 Mio. Betriebsstunden über mindestens zwei Jahre mit unterschiedlichen Einrichtungen einschließlich Sicherheitsanalyse, detaillierter Dokumentation auch kleinerer Änderungen während der Betriebszeit.	
sehr empfohlen	empfohlen		

Bild 5.16: Zuständigkeiten und Maßnahmenübersicht bei Verifikation und Validierung

Wie bereits in vorhergehenden Abschnitten kurz eingeführt, müssen im Technischen Sicherheitsbericht mindestens zu den folgenden Bereichen Informationen enthalten sein:

- Eine Einleitung mit einer kurzen Systemübersicht, in der die technischen Sicherheitsprinzipien, auf denen die Systemsicherheit beruht, zusammengefasst sind.
- Der Nachweis des korrekten funktionalen Systemverhaltens. Dabei ist auf die Systemarchitektur, Teilsysteme und Komponenten, die Definition der Schnittstellen, die Erfüllung von Anforderungen sowie die Einhaltung von rechtlichen Grundlagen einzugehen.
- Die sicherheitsbezogenen Anwendungsbedingungen sind herauszustellen, einschließlich der Betriebs- und Instandhaltungsprozesse. Das gilt ebenso für vorausgesetzte Anwendungsbedingungen (getroffene Annahmen) für die Implementierung und den Betrieb.
- Darstellung der Ausfallauswirkungen unter Berücksichtigung der Unabhängigkeit von Betrachtungseinheiten, die Auswirkung und Offenbarung von Ausfällen sowie der Prozesse nach der Ausfalloffenbarung.
- Die Darstellung des Systembetriebs mit externen Einflüssen unter Berücksichtigung von Umgebungsparametern.
- Der Nachweis der Sicherheitserprobung unter Betriebsbedingungen.

Zusammenfassungen und Referenzierungen auf Dokumente stellen eine übliche Vorgehensweise dar; insbesondere wenn typzugelassene Teilsysteme Anwendung finden, kann auf die Typzulassung verwiesen werden. Bestehen z.B. eingeführte Betriebs- und Instandhaltungsvorschriften bei einem Unternehmen, welche in gleicher Weise mehrfach angewendet werden, kann auf die entsprechende Dokumentation verwiesen werden [EN 50129].

5.2.3.5 Ergänzungen

Beziehungen zu anderen Sicherheitsnachweisen sollen die Beziehungen zu Nachweisen, Gutachten und Typenzulassungen der untergeordneten Teilsysteme und Komponenten sowie zu den Nachbarsystemen aufzeigen. Werden Komponenten oder Teilsysteme mit einer Typenzulassung eingesetzt, hat der Betreiber bzw. das Eisenbahnunternehmen nachzuweisen, dass die zugelassenen und zum Einsatz vorgesehenen Teilsysteme und Komponenten im konkreten Anwendungsfall konform zur Typenzulassung eingesetzt und die Sicherheitsanforderungen und Einsatzbedingungen der Typenzulassung erfüllt sind.

In einer abschließenden Zusammenfassung muss bestätig werden, dass das Vorhaben den maßgebenden gesetzlichen Grundlagen entspricht und ein entwickeltes und ausgeführtes System den sicheren Betrieb erlaubt.

6 VALIDATION DER METHODE FÜR FAHRZEUGAUTARKE ORTUNG

Auf Grundlage des methodischen Konzepts für eine durchgängige Sicherheitsuntersuchung in Verbindung mit technischem Anwendungsbezug wird im Folgenden exemplarisch eine Sicherheitsuntersuchung durchgeführt und durch eine Verfügbarkeitsbetrachtung ergänzt. Als technischer Betrachtungsgegenstand wird die fahrzeugautarke Ortung (Zugspitzenortung) aus dem DemoOrt-Projekt herangezogen und mit dem Betriebsprozess des Zugleitbetriebs verknüpft. Im Vordergrund der Betrachtung steht eine automatisierte und sicherheitsrelevante Unterstützung des Zugleitbetriebs auf Nebenbahnen. Auf die Innovationen der Zugintegritätsprüfung wird im Ausblick eingegangen.

6.1 Exemplarische Sicherheitsuntersuchung

Ausgehend von der semiformalen Systemdefinition des Ortungssystems DemoORT werden die Systemgrenzen der Zugspitzenortung festgelegt und der Verkehrsprozess des Zugleitbetriebs auf Nebenbahnen mittels formaler Modellierung ergänzt. Als Basis dient hierbei das PROFUND-Konzept, welches in [Slovak 2007] detailliert vorgestellt ist.

Aus der formalen Prozessbildung können Sicherheitsfunktionen abgeleitet werden, die in die Gefährdungsidentifikation einfließen. Das zugehörige methodische Vorgehen wurde bei der Erstellung der generischen Gefährdungsliste für das Projekt „EURO-Interlocking“ angewendet und tiefer gehend in [Drewes/May 2007] erläutert.

Die potenziellen sicherheitsrelevanten Funktionsbeeinträchtigungen werden mit Hilfe einer FMEA beurteilt und – soweit möglich – anschließend einer FMECA gemäß [EN 60812] unterzogen. Zur Quantifizierung würde sich auch die Anwendung von Störungsbäumen [IEC 61025] anbieten, die Transferierung der Daten ohne Werkzeugunterstützung könnte hierbei aber eine Fehlerquelle bilden, die zu vermeiden ist. Werkzeuge mit einer automatisierten Transfermöglichkeit sind aber erhältlich und sollten unterstützend für Projekte dieser Art herangezogen werden [Schneeweiss 1999].

Die Ergebnisse der Gefährdungsfolgen werden einer Risikoabschätzung unterzogen. Dabei spielen insbesondere die jeweilige Systemanwendung und die Unternehmensphilosophie entscheidende Rollen.

Als Abschluss erfolgt die Bewertung des Systemrisikos durch Abgleich des Risikoakzeptanz-kriteriums mit dem Nachweis mindestens gleicher Sicherheit anhand eines Bezugssystems.

6.1.1 Situationsabgrenzung

Das fahrzeugautarke Ortungssystem stellt die Basis zur Positionsbestimmung eines Schienen-fahrzeuges auf dem Gleis dar. Die durch das sicherheitsrelevante Ortungssystem erzielbaren Ortungsinformationen werden weiteren sicherheitsrelevanten Systemen zur Verfügung gestellt, wodurch das Ortungssystem Sicherheitsverantwortung trägt. Eine Analyse und der Nachweis der

Sicherheit sind nach CENELEC somit für eine Zulassung bzw. Zertifizierung erforderlich [EN 50126].

6.1.2 Angewandte Systemdefinition und -abgrenzung

Betrachtet wird ein sicherheitsrelevantes fahrzeugautarkes Ortungssystem für Schienenfahrzeuge, das dem DemoORT-System ohne Referenzmesssystem (vgl. Abschnitt 3.5.2) entspricht.

Die Definition des Systems mit der Darstellung und Festlegung der Systemgrenzen wird durch Bild 6.1 eingegrenzt. In der exemplarischen Anwendung sind entsprechend die Teilsysteme des Wirbelstromsensors (Sensor 1 und 2), des Streckenatlasses, des „Map-Matching“, der Sensordatenfusion und des GNSS zu berücksichtigen.

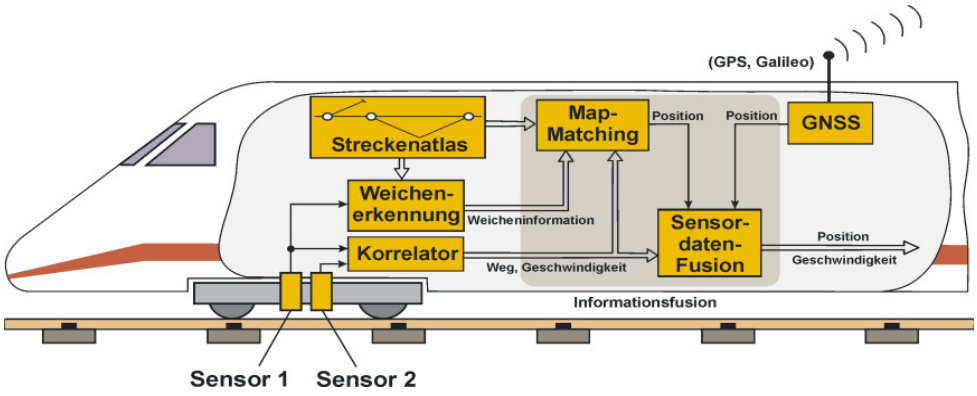

Bild 6.1: Systemaufbau und -grenzen DemoORT (ohne Referenzmesssystem)

Durch Fusion der Ortungsinformation können Position und Geschwindigkeit des Fahrzeugs auch bei vorübergehendem Ausfall eines der Teilsysteme (z.B. kein ausreichender Satellitenempfang) bestimmt werden, da die Ortungsinformation noch über andere Sensoren zuverlässig bestimmt werden kann. Position und Geschwindigkeit werden mit einer spezifizierten Messunsicherheit und Zuverlässigkeit über eine Schnittstelle bereitgestellt und können von übergeordneten (Sicherungs-) Systemen, die außerhalb des hier betrachteten Rahmens liegen, eingelesen und verarbeitet werden [Geistler 2006].

Angelehnt an die Struktur des multisensorischen Ortungssystems DemoOrt wird die funktionale Systemstruktur in Form eines Kanal-Instanzen Netzes [Schnieder 1999] zur Systemdefinition mit Darstellung der Systemgrenzen umgesetzt (Bild 6.2). Der dargestellte Definitionsbereich des Systems erstreckt sich von der Sensierung der Informationen durch die im System integrierten Sensoren bis zur Bereitstellung einer sicheren Positions- und Geschwindigkeitsinformation für weitere Systeme, wodurch gleichzeitig der Nutzungszustand dargestellt wird.

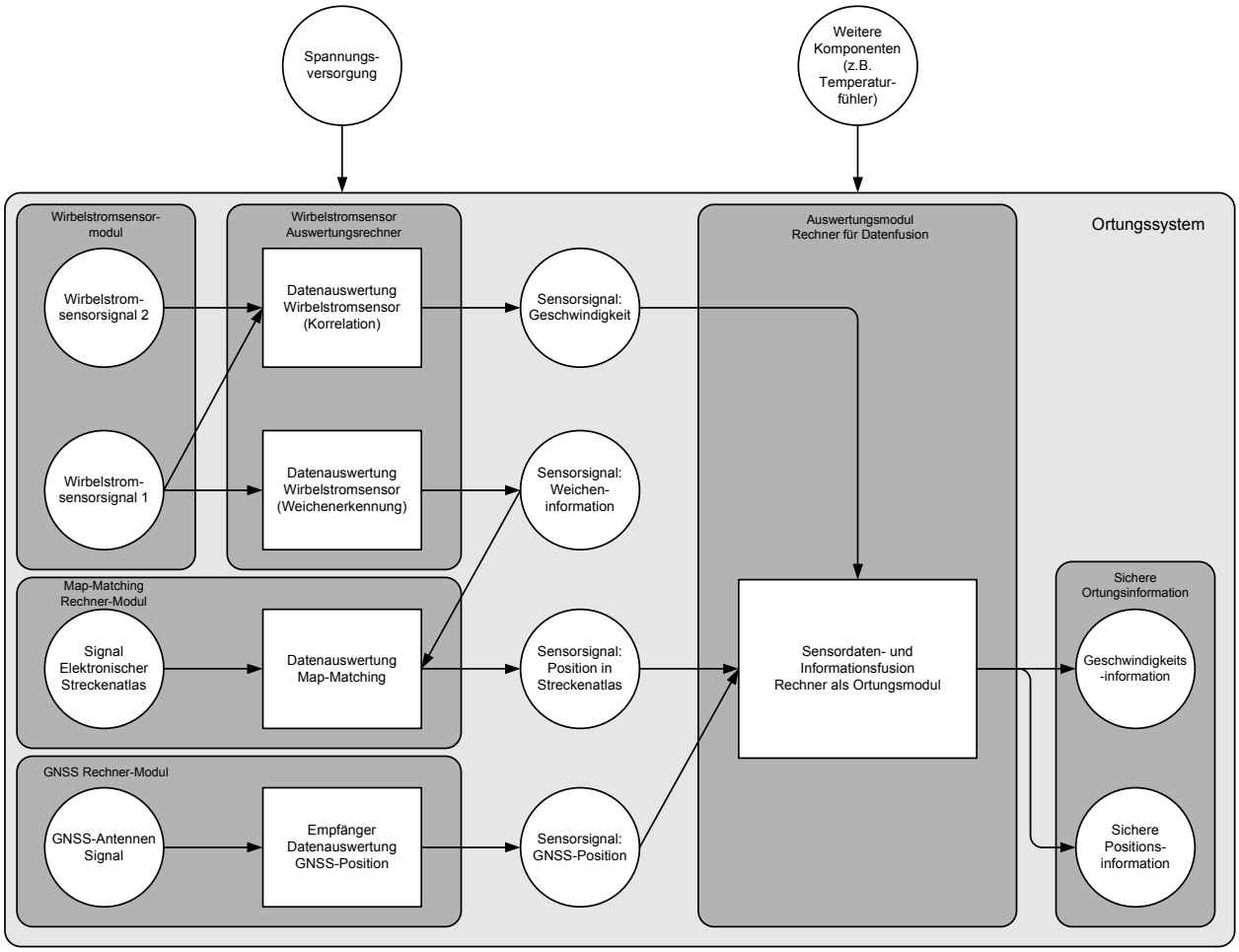

Bild 6.2: Systemdefinition des modularen DemoORT-Ortungssystem als Kanal-Instanzen Netz

Das Ortungssystem nach DemoORT lässt sich in sechs relevante Systemmodule (siehe dunkelgraue Kästen in Bild 6.2) unterteilen:

Das Wirbelstromsensormodul besteht aus zwei in einem Bauteil integrierten Wirbelstromsensoren. Die sensierten Informationen werden zur Datenauswertung an einen Auswertungsrechner über ein Kommunikationsmodul übertragen, in dem nachfolgend die Detektierung der überfahrenen Weichen unter Berücksichtigung der Daten aus dem Streckenatlas erfolgt sowie durch Korrelationsauswertung der beiden Sensorsignale die Geschwindigkeit und der zurückgelegte Weg berechnet wird. In einem weiteren Rechner wird die elektronische Streckenkarte verwaltet und das Map-Matching, der Vergleich der sensierten Weicheninformationen mit den Streckenatlasdaten, ausgeführt. Das GNSS-Rechner-Modul besteht aus der GNSS-Antenne und dem zugehörigen Satellitenempfänger, von dem aus die errechnete GNSS-Position als Ausgangsgröße übertragen wird. Aus allen vorgenannten Modulen werden die Daten in einem Auswertungsrechnermodul fusioniert und zu einer sicherheitsrelevanten Ortungsinformation verarbeitet. Als weitere Ausgangsinformation kann die Fahrzeuggeschwindigkeit zur Verfügung gestellt werden.

Nicht direkt dem System zugehörig sind die Spannungsversorgung sowie weitere Komponenten für den Systembetrieb, wie z.B. ein Temperaturmanagement, eine unterbrechungsfreie Spannungsversorgung (USV-Modul), das Schrankgehäuse für die Rechner etc. Diese externen Systemkomponenten werden an dieser Stelle nicht weiter berücksichtigt; in einer spezifischen Sicherheitsanalyse wäre eine Berücksichtigung hingegen obligatorisch.

6.1.3 Definition der Kontakt- oder Schnittstellen

a) Eine Bedienung des Ortungssystems durch Personal erfolgt nur im Wartungs- oder Reparaturbetrieb. Auf die Mensch-Maschine-Kontaktstelle kann während des Betriebes nicht zugegriffen werden.

b) Zur Instandhaltung des Ortungssystems besteht Zugriff über eine Programmierkontaktstelle zu den Rechnermodulen.

Technische Kontaktstellen:

a) Interne Kontaktstellen bestehen zwischen den einzelnen Modulen über Buskommunikationsmittel, über die der Dateninformationsaustausch stattfindet. Aufgrund der Anordnung als abgeschlossenes System sind die internen Kontaktstellen gegen ungewollten Zugriff geschützt.

b) Zwischen den fahrzeugseitigen Außenkomponenten, wie Wirbelstromsensormodul und GNSS-Antenne, und den inneren Systemkomponenten mit Auswertungsrechnern werden die Schnittstellen mit Hilfe von gesicherten Buskommunikationsmitteln verknüpft. Aufgrund der geringen Ströme können EMV-Auswirkungen auf die Fahrzeugsteuerung vernachlässigt werden. Die Kabel sind weitestgehend gekapselt auszuführen, wodurch Störungseinflüsse vernachlässigbar sind.

c) Zwischen dem Schienenfahrzeug und den inneren Systemkomponenten besteht eine Kontaktstelle über gesicherte Buskommunikationsmittel mit einer Spannungsversorgung, die an dieser Stelle nicht betrachtet wird.

d) Ausgangsinformationen wie die sichere Positions- und Geschwindigkeitsinformation werden über eine nicht weiter spezifizierte Schnittstelle sekundären Systemen zur Verfügung gestellt.

6.1.4 Angewandte Prozessdefinition

Für die spätere vergleichende Betrachtung durch Nachweis der mindestens gleichen Sicherheit – entsprechend EBO §2 (2) – wird als Referenzsystem exemplarisch der Zugleitbetrieb auf Nebenbahnen herangezogen. Dem manuell nicht technisch gesicherten System sind Betriebsregeln zugeordnet, wobei der Zugleitbetrieb ohne Signalisierung für die weitere Betrachtung als Betriebsverfahren herausgestellt wird. Wie bereits angeführt, wird der Zugleitbetrieb (vgl. Abschnitt 2.5.2.2), der in Kombination mit dem Ortungssystem sicherheitsrelevant Anwendung findet, als betrachtet. Umgesetzt in die im Zugleitbetrieb realen Kommunikationsstrukturen wird in Bild 6.3 das Modell des relevanten Kommunikationsprozesses zwischen dem Zugleiter (ZL) und dem Eisenbahnfahrzeugführer (Ef) als Petrinetz aufgestellt. Wie o.a. werden die Positionsinformationen des Zuges fernmündlich durch den Ef an den ZL übertragen, der mittels dieser Informationen eine Fahrerlaubnis für den Zug generiert und ebenfalls fernmündlich an den Ef zurück übermittelt.

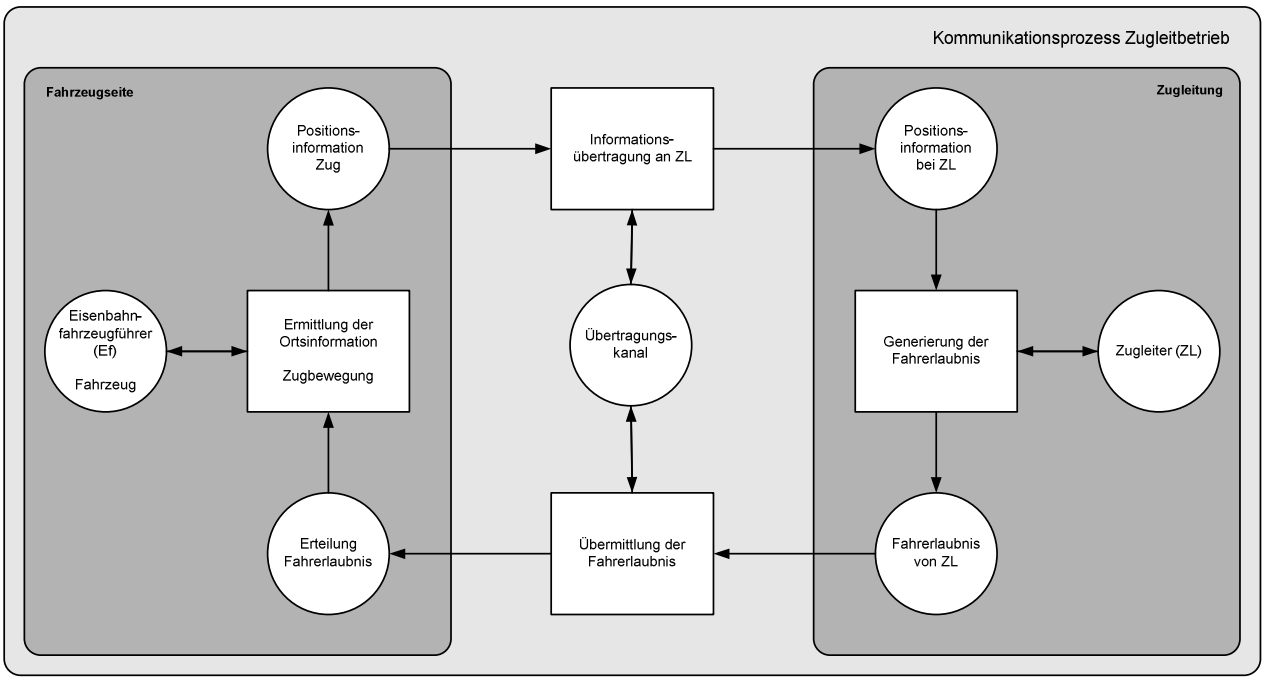

Bild 6.3: Prozessmodell des Zugleitbetriebs als Petrinetz

Um das innovative Ortungssystem in den Prozess zu integrieren wird das Modell der funktionalen Systemdefinition mit dem Prozessmodell verknüpft. Als Basis dient hierbei der PROFUND-Ansatz nach [Slovak 2007].

Im ersten Betrachtungsansatz wird das sicherheitsrelevante Ortungssystem als überlagertes „Rucksacksystem“ aufgefasst. Der eigentliche Betriebsprozess inkl. aller Kommunikationen bleibt unverändert, so dass eisenbahnbetriebliche Abläufe nicht geändert werden müssen. Lediglich die sichere Positionsinformation des Zuges wird ergänzend und somit redundant durch das Ortungssystem an den ZL zur Plausibilisierung der durch den Ef ermittelten Informationen

übertragen (Bild 6.4). Die sichere Positionsinformation des Systems wird durch den ZL mit den fernmündlichen Informationen des Ef verglichen. Im Fall einer Abweichung wird der ZL keine Fahrerlaubnis an den Ef übermitteln.

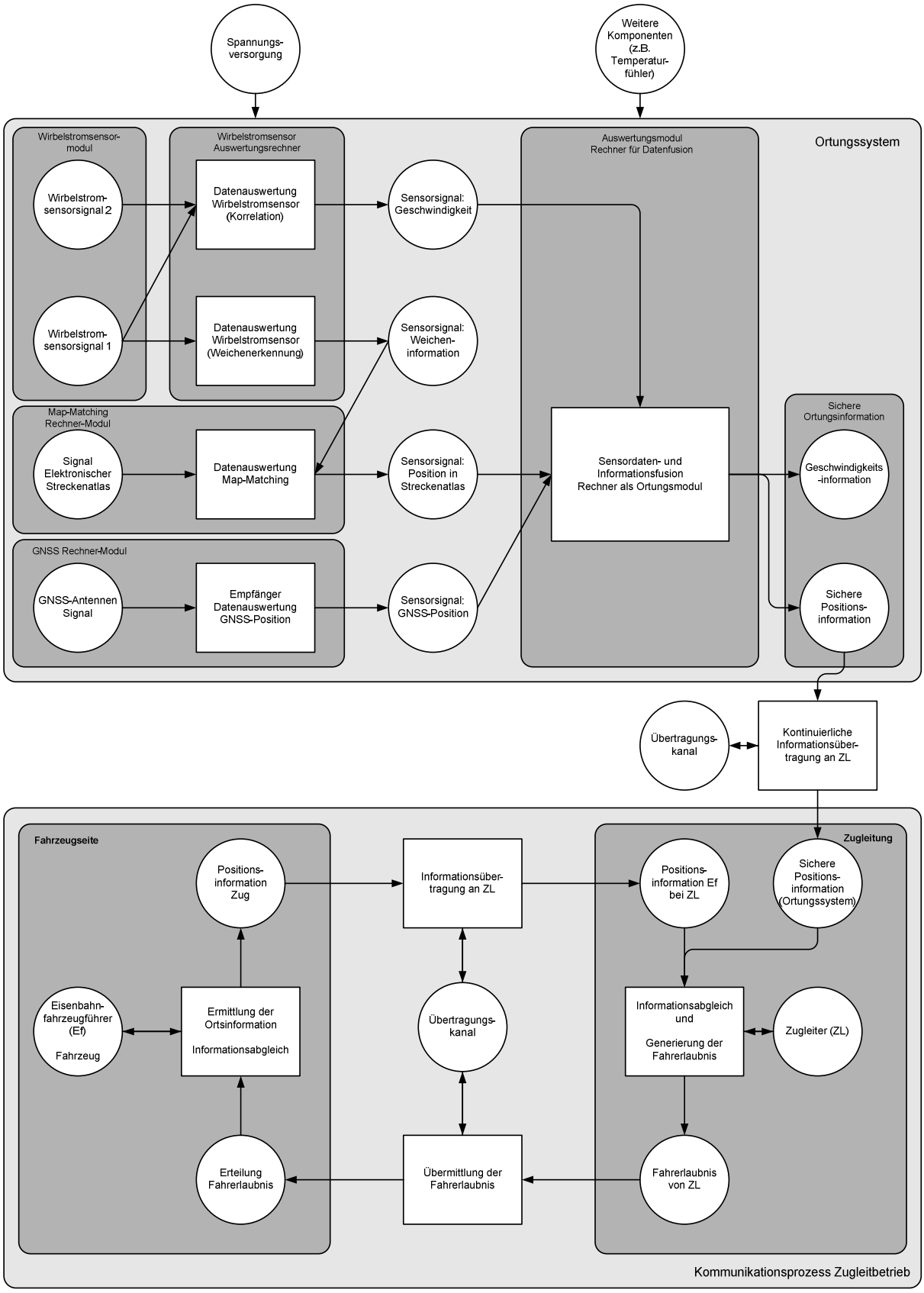

Bild 6.4: Modell des Ortungssystems als redundante Positionsinformation im Zugleitbetrieb

Im zweiten Betrachtungsansatz wird das sicherheitsrelevante Ortungssystem als alleiniges Positionsinformationssystem des Fahrzeuges aufgefasst. Der Betriebsprozess wird vereinfacht, so dass der Ef keine Positionsinformationen mehr an den ZL übermitteln muss, wodurch eine Arbeitserleichterung und somit in Bezug auf menschliches Fehlverhalten eine Risikoreduktion erreicht wird. Ein potenzielles technisches Versagen muss an der Stelle berücksichtigt und analysiert werden (Bild 6.5).

Bilder 6.4 und 6.5 stellen die beiden Betrachtungsansätze als Petrinetz-Modelle dar und sind selbst jeweils verfeinerte Darstellungen des Modells aus Bild 6.5.

Die nachfolgende Gefährdungsidentifikation kann in Abhängigkeit der prozessbezogenen Systemdefinition sehr umfangreich ausfallen. Entscheidend sind hierbei die Betrachtungstiefe und Art des eigentlichen Betriebsprozesses mit der Umsetzung der Kommunikationsstrukturen. Für die weiterführende Betrachtung sei an dieser Stelle auf eine Vielzahl von Projektarbeiten mit der Erstellung umfangreicher Prozessmodelle verwiesen: [Ständer et al. 2007], [Drewes/May 2007], [Baier/Enning 2006].

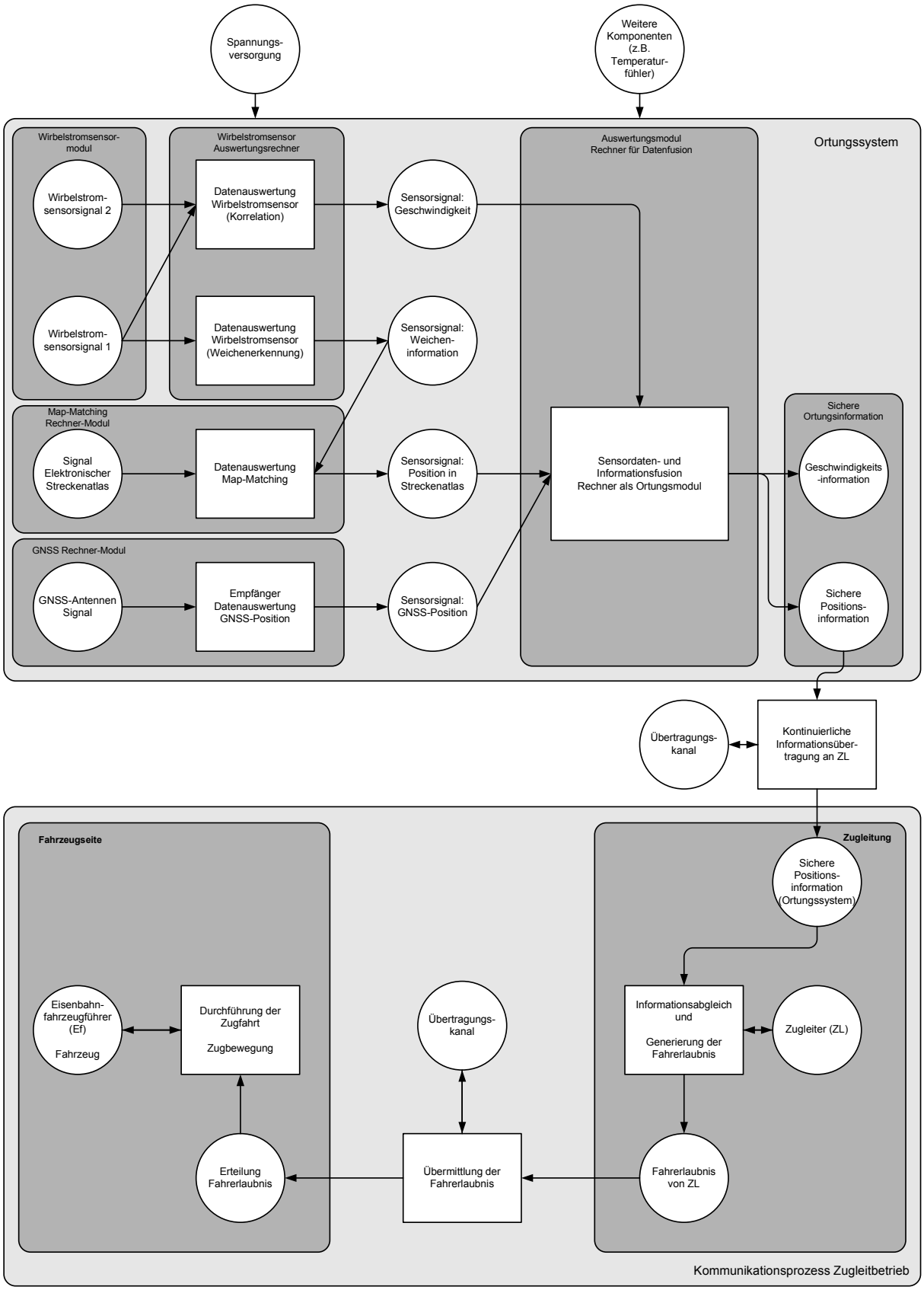

Bild 6.5: Modell des Ortungssystems mit integrierter Positionsinformation im Zugleitbetrieb

6.1.5 Gefährdungsidentifikation

Bezogen auf ein in den Betriebsprozess integriertes oder auch überlagertes Ortungssystem als zusätzliche sicherheitsrelevante Informationsquelle für die Zugposition kann als Unfallart die Entgleisung ebenfalls vernachlässigt werden, da Geschwindigkeitsinformationen aus dem Ortungssystem nicht sicherheitsrelevant im Betriebsablauf Anwendung finden. Die Betrachtung des Zugleitbetriebs selbst soll hierbei unberücksichtigt bleiben. Aus diesem Grund beschränkt sich die nachfolgende Analyse und Identifikation der Gefährdungen lediglich auf die Kollision als Unfallart.

Unter Anwendung der Prozessmodellteile aus den Bildern 6.4 und 6.5 mit Berücksichtigung des generischen Regelkreises des Betriebsprozesses (Bild 5.4) können die vier relevanten Prozessschritte des Betriebsprozesses zur weiteren Analyse in die nachfolgende Gefährdungstabelle eingetragen werden – vgl. Bild 6.6 ($I_{Prozess}$). Als zu berücksichtigende Ressource wird die „sichere Positionsinformation des Ortungssystems“ herangezogen, da diese in Bezug auf das herkömmliche Betriebsverfahren hinzugezogen wird und sicherheitsrelevante Auswirkungen hervorrufen könnte. Die Ressourcen ZL und Ef haben ebenfalls Sicherheitsrelevanz, da sie für Weitergabe und z.T. auch für Verarbeitung der Positionsinformationen verantwortlich sind und somit sicherheitsrelevante Fehler verursachen können. Spätestens bei einer potenziellen Änderung des Betriebsverfahrens müssen dessen Eigenschaften ebenfalls berücksichtigt werden, da sich die sicherheitsrelevanten Aufgaben des Personals verändern [Hinzen 1993].

In der Gefährdungstabelle (Bild 6.6) werden die relevanten Betriebsprozessschritte jeweils mit der zugehörigen Ressource tabellarisch in Zusammenhang gebracht und je ein Ausfall oder Fehler des Prozessschrittes in Verbindung mit der sichereren Positionsinformation analysiert. In allen vier Fällen wären als Folgen Unfälle durch Kollision zweier Schienenfahrzeuge möglich, welche in der Zuordnung A bis D dargestellt sind [Drewes/May 2007].

Die ergänzenden Bezeichnungen (Kreise mit Nummernschema) dienen der späteren Zuordnung in der FMECA (vgl. Bild 6.10). $I_{Ressource}$ und $I_{Prozess}$ stellen die Systemmerkmale dar. II und IV teilen sich die kausalen Abhängigkeiten der potenziellen Fehler und der Fehlerursachen. III hingegen stellt die potenzielle Fehlerfolge, den Unfall dar. Erst in Kombination aller Faktoren ist eine potenzielle Gefährdung eindeutig definiert.

Das methodische Vorgehen zur Gefährdungsidentifikation basiert auf den Ergebnissen des Projekts „Eurointerlocking“ des internationalen Eisenbahnverbandes (UIC); weiterführende Informationen sind in [Drewes/May 2007] dokumentiert.

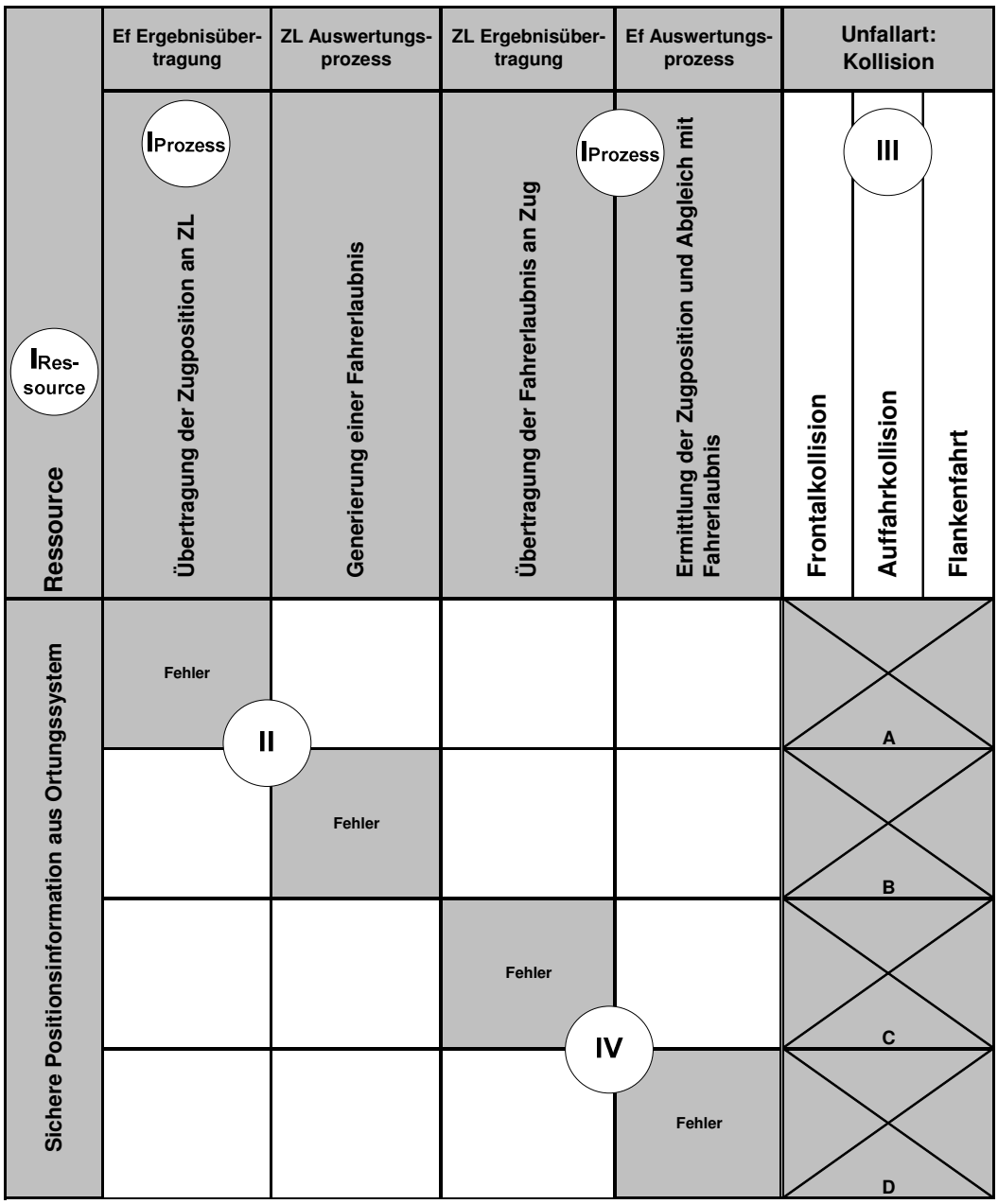

Bild 6.6: Gefährdungstabelle für den Zugleitbetrieb mit Ortungssystem

Die in Bild 6.6 aufgestellten tabellarischen Zusammenhänge der Gefährdungen werden nachfolgend in Textform kausal zusammengestellt und als Systemgefährdungen identifiziert.

Identifizierte Gefährdungen:

A: Potenzielle Kollision zweier Züge aufgrund Übertragung einer falschen Positions-informationsmeldung an den Zugleiter. (Diese Gefährdung ist nur beim 1. Betrachtungsfall mit „Rucksacksystem“ relevant).

B: Potenzielle Kollision zweier Züge aufgrund falscher Generierung einer Fahrerlaubnis aus den Positionsinformationen.

C: Potenzielle Kollision zweier Züge aufgrund falscher oder fehlerhafter Übertragung der Fahrerlaubnis auf Basis der Positionsdaten.

D: Potenzielle Kollision zweier Züge aufgrund Abgleichs der Fahrerlaubnis mit einer falschen eigenen Positionsinformation durch den Ef. (Diese Gefährdung ist nur beim 1. Betrachtungsfall mit „Rucksacksystem“ relevant).

Aus den identifizierten Gefährdungen wird deutlich, dass sich eine als „sicher“ einzustufende Positionsinformation des Ortungssystems bei unerkannter Fehlerhaftigkeit sicherheitsrelevant auswirken kann. Auf Grundlage der falschen Positionsinformation kann nachfolgend einem Zug eine „falsche“ Fahrerlaubnis generiert werden. Bei der Übertragung einer vermeintlich „richtigen“ Fahrerlaubnis kann in Verbindung mit einer falschen Positionsinformation ebenfalls als Folge eine Kollision (unerwünschter Zustand) entstehen. Das gilt gleichermaßen für den Fall, dass der Ef zu einer Zugfahrt veranlasst wird, indem er die Fahrerlaubnis mit einer unerkannt falschen eigenen Position abgleicht.

Durch Umstrukturierung des Satzbaus der genannten identifizierten Gefährdungen und Schadensfolgen lässt sich in Form einer Zusammenfassung eine übergeordnete Sicherheitsanforderung ableiten. Alle einem Prozess zugeordneten identifizierten Gefährdungen haben stets eine Sicherheitsanforderung gemeinsam. Das methodisches Vorgehen sowie vertiefende Erläuterungen sind in [Drewes/May 2007] enthalten.

Sicherheitsanforderung:

Das Ortungssystem muss sicherstellen, dass keine falschen oder fehlerhaften Positionsinformationen an ein übergeordnetes System abgegeben werden.

Die Begriffe „falsch“ und „fehlerhaft“ müssen entsprechend nach den Grenzen des Vertrauensintervalls des Ortungssystems definiert und in der Systemanforderungsspezifikation – vgl. V-Modell – berücksichtigt werden. Bezogen auf ein Ortungssystem ist der sichere Zustand erreicht, wenn der wahre Wert der Positionsinformation innerhalb des vorgegebenen Vertrauensintervalls liegt [Kiriczi 1996].

Mit Hilfe der identifizierten Gefährdungen, die durch das Ortungssystem auf externe Systeme entstehen können, wird im folgenden Abschnitt das System nach potenziellen Ursachen und Folgen untersucht.

6.1.6 Exemplarische Ursachen- und Folgenanalyse

Die nachfolgende exemplarische Betrachtung konzentriert sich auf eine Kombination aus System- und Konstruktions-FMEA des Ortungssystems. Bei der Erarbeitung der Analyse werden an FMEA-Formblätter angelehnte Tabellen herangezogen.

Auf Basis des Modells der Systemdefinition (Bild 6.2) als Kanal-Instanzen Netz kann die Analysestruktur des Ortungssystems (Bilder 6.7 und 6.9) mit der Definition der Funktionen der Strukturelemente geeignet generiert werden. Mit Hilfe der Analysestruktur mit der jeweiligen Zuordnung der Teilsysteme und Funktionen zu potenziellen Ursachen und Folgen kann eine Einarbeitung in die FME(C)A-Formblätter erfolgen. Die baumartige Analysestruktur ist in Betrachtungsstufen unterteilt, deren erste bei den übergeordneten Systemkomponenten auf Ursachenebene beginnt. Die sich daraus ergebenden Funktionen (Fehler / Ausfall) wandern bei der zweiten Betrachtungsstufe in die Ursachenebene usw.

Im ersten Ansatz (Bild 6.7) wird die erste Betrachtungsstufe des Systems analysiert.

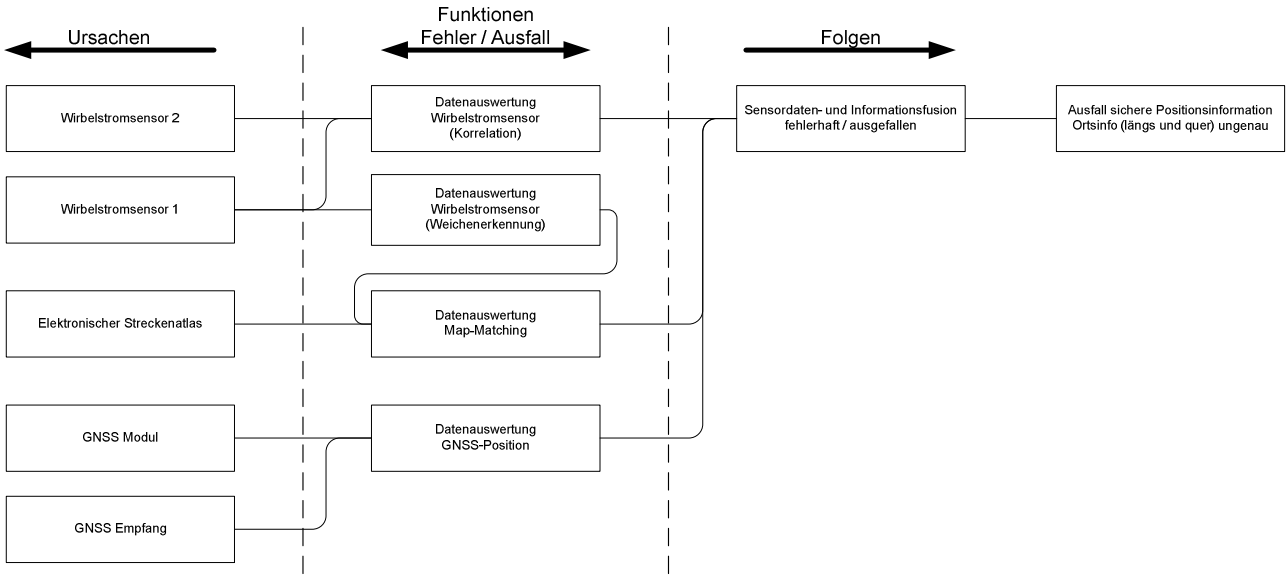

Bild 6.7: FMEA-Analysestruktur (1. Betrachtungsstufe) für das Ortungssystem DemoOrt

Mit Hilfe der Analysestruktur der ersten Betrachtungsstufe lässt sich das nachfolgende FMEA-Formblatt (Bild 6.8) ausfüllen. Die Nummerierung (1-1.1 ff.) der zu untersuchenden Systemteile dient als Basis für die spätere Bewertung. Die erste Ziffer (1-x) stellt dabei die Betrachtungsstufe der FMEA dar. Die weitere Ziffernfolge gilt für die Unterscheidung der Teilsysteme.

	Fehlermöglichkeits- und -einflussanalyse (FMEA)								
	Konstr.-FMEA	Prozess-FMEA X	System-FMEA					Gesamtsystem	
	Bestätigung durch betroffene Stellen	Kurzzeichen Teilnehmer		Projektleiter gesehen				Sicherheitsrelevantes Ortungssystem nach DemoOrt	
Systeme/Merkmale	Potentielle Fehler	Potentielle Fehlerfolgen	Potentielle Fehlerursachen	DERZEITIGER ZUSTAND					Empfohlene Maßnahme
				Ergänzungen	A	B	E	RPZ	
1-1.1 Datenauswertung Wirbelstromsensor (Korrelation)	Keine Daten-auswertung	Keine oder fehlerhafte Sensordaten- und Informationsfusion	Ausfall Wirbelstromsensor 1 und / oder Wirbelstromsensor 2	Für die Generierung der sicheren Positionsinformation wird die berechnete Geschwindigkeit nicht genutzt.	5	1	1	5	Keine weitere Maßnahme erforderlich.
1-2.1 Datenauswertung Wirbelstromsensor (Weichen-erkennung)	Keine Daten-auswertung	Falsche Datenauswertung Map-Matching	Ausfall Wirbelstromsensor 1	Durch Korrelationsprüfung der Wirbelstromsensordaten können nur kein und keine falschen Daten gesendet werden.	5	1	1	5	Keine weitere Maßnahme erforderlich.
1-3.1 Datenauswertung Map-Matching	Falsche Daten-auswertung	Fehlerhafte Sensordaten- und Informationsfusion	Falsche Datenauswertung Wirbelstromsensor (Weichenerkennung)	Durch Korrelationsprüfung der Wirbelstromsensordaten können nur kein und keine falschen Daten gesendet werden.	5	1	1	5	Keine weitere Maßnahme erforderlich.
1-3.2 Datenauswertung Map-Matching	Falsche Daten-auswertung	Fehlerhafte Sensordaten- und Informationsfusion	Elektronischer Streckenatlas fehlerhaft	Der Atlas wird nach Erstellung und Änderungen stets validiert.	1	8	5	40	Validierung des Streckenatlasses nach Änderungen ist als Prozess verpflichtend einzuführen.
1-4.1 Datenauswertung GNSS-Position	Falsche Daten-auswertung	Fehlerhafte Sensordaten- und Informationsfusion	GNSS-Modul sendet falsche Daten	Hochpräziser Empfänger wird verwendet.	2	8	6	96	Sehr genauen und hoch verfügbaren Empfänger verwenden.
1-4.2 Datenauswertung GNSS-Position	Keine Daten-auswertung	Fehlerhafte Sensordaten- und Informationsfusion	Kein GNSS Empfang	Kein Empfang von Daten wird erkannt und wirkt verfügbarkeitseinschränkend.	4	5	1	20	Sehr genaue und hoch verfügbare Redundanz anderer Sensoren verwenden.

Bild 6.8: FMEA Formblatt für das Ortungssystem (1. Betrachtungsstufe)

Nach Durchführung einer ersten Risikobeurteilung durch die subjektive Einschätzung der Parameter zur Berechnung der Risikoprioritätszahl (RPZ) wurden Maßnahmen und Lösungsvorschläge bezüglich der priorisierten Risiken empfohlen. Auf eine tiefer gehende Betrachtung der Vermeidungs- und Entdeckungsmaßnahmen wird aufgrund des exemplarischen Charakters der Analyse verzichtet.

Bei komplexeren Systemen bzw. tiefer gehenden Systemstrukturen sind die zu betrachtenden Funktionen so zu verschieben, dass eine mehrstufige FMEA entsteht. Die potenziellen Fehlerfolgen der ersten Betrachtungsstufe lassen keine Aussagen über Maßnahmen zur Abwehr der im vorhergehenden Abschnitt analysierten Gefährdungen in Bezug auf den Betriebsprozess zu. Deshalb wird im Folgenden eine zweite Betrachtungsstufe der FMEA analysiert.

Auch dazu wird auf Grundlage des Modells der Systemdefinition (Bild 6.2) die Analysestruktur in der zweiten Betrachtungsstufe des Ortungssystems generiert.

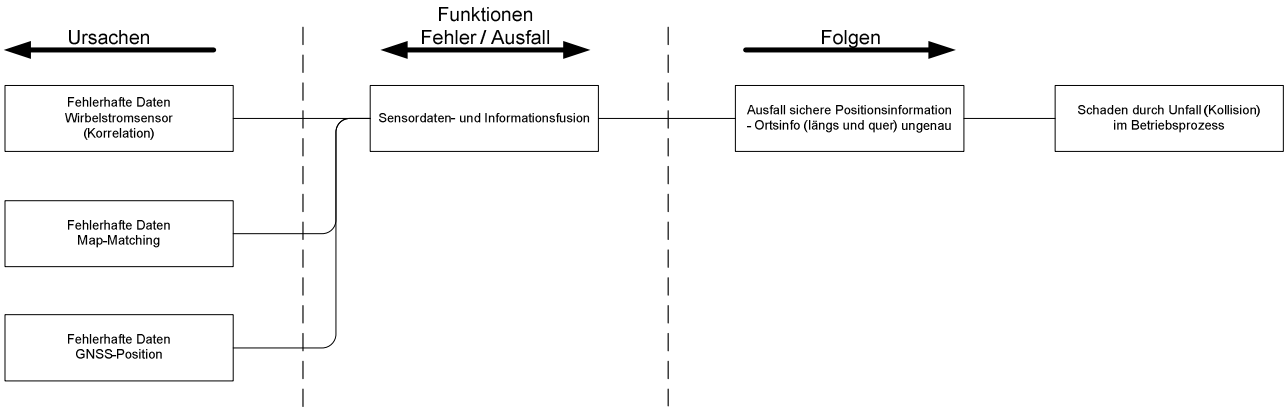

Bild 6.9: FMEA Analysestruktur (2. Betrachtungsstufe) für das Ortungssystem DemoOrt

Ebenfalls lässt sich mit Hilfe der Analysestruktur der zweiten Betrachtungsstufe das nachfolgende FMEA Formblatt erstellen (Bild 6.10). In diesem Fall ist die potenzielle Gefährdung als Schaden – Kollision zweier Züge im Betriebsprozess – bereits berücksichtigt.

Durch die ergänzenden Bezeichnungen (Kreise mit Ziffern I bis IV) wird die Zuordnung der Systemmerkmale und Gefährdungspotenziale aus der Gefährdungsidentifikation deutlich (vgl. Abschnitt 6.1.5).

	Fehlermöglichkeits- und -einflussanalyse (FMEA)								
	Konstr.-FMEA	Prozess-FMEA X	System-FMEA						
	Bestätigung durch betroffene Stellen	Kurzzeichen Teilnehmer		Projektleiter gesehen					
					Gesamtsystem Sicherheitsrelevantes Ortungssystem nach DemoOrt				I Res-source
Systeme/Merkmale I Pro-zess	Potentielle Fehler II	Potentielle Fehlerfolgen III	Potentielle Fehlerursachen IV	DERZEITIGER ZUSTAND Ergänzungen	A	B	E	RPZ	Empfohlene Maßnahme
2-1.1 Sensordaten- und Informationsfusion	Keine oder fehlerhafte Sensordaten und Informations-fusion	Ausfall sichere Positionsinformation (potenzielle Kollision)	Fehlerhafte Daten Wirbelstromsensor (Korrelation)	Für die Generierung der sicheren Positionsinformation wird die berechnete Geschwindigkeit aus der Korrelation nicht benötigt.	5	1	1	5	Keine weitere Maßnahme erforderlich.
2-1.2 Sensordaten- und Informationsfusion	Keine oder fehlerhafte Sensordaten und Informations-fusion	Ausfall sichere Positionsinformation (potenzielle Kollision)	Fehlerhafte Daten Map-Matching (mit Weichen-identifikation)	Fehlerhafte Daten können eine falsche Zugpositon zur Folge haben.	2	8	5	80	Die Aktualität der Karte und die Auswertung sind kontinuierlich zu prüfen. Berechnung der Sensordaten redundant auszulegen und erst nach Abgleich als sichere Positions-information zu senden.
2-1.3 Sensordaten- und Informationsfusion	Keine oder fehlerhafte Sensordaten und Informations-fusion	Ausfall sichere Positionsinformation (potenzielle Kollision)	Keine oder fehlerhafte Daten GNSS-Position	Keine GNSS-Daten werden durch andere Sensoren redundant abgedeckt. Fehlerhafte Daten können eine falsche Zugpositon zur Folge haben.	4	8	4	128	Hochverfügbare und sichere Komponenten sind im System zu verwenden. Berechnung der Sensordaten sind redundant auszulegen und erst nach Abgleich als sichere Positions-information zu senden.

Bild 6.10: FMEA Formblatt für das Ortungssystem (2. Betrachtungsstufe)

Auch in der zweiten Betrachtungsstufe der FMEA wurde eine erste Risikobeurteilung durch die subjektive Einschätzung der Einflussgrößen inkl. Berechnung der Risikoprioritätszahl (RPZ) durchgeführt, was methodisch einer FMECA entspricht.

6.1.7 Angewandte Risikoabschätzung

In den Ergebnissen (Bilder 6.8 und 6.10) sind die Risikoprioritätszahlen 80, 96 und 128 auffallend. Da bezüglich der ermittelten Gefährdungen das Grenzrisiko damit intuitiv überstiegen ist (vgl. Abschnitt 5.2.1.6), ist die Risikoabschätzung in diesen Fällen näher zu untersuchen.

Herausgearbeitete FMEA Nr. 2-1.2
Keine oder fehlerhafte Sensordaten- und Informationsfusion
(FMEA Nr. 1-4.1 als Ursache bereits enthalten):

Risikoeinschätzung:

- Basierend auf potenziell falschen oder fehlerhaften Daten aus dem Map-Matching könnte eine falsche Zugposition bei der Sensordaten- und Informationsfusion generiert werden.

Maßnahmen:

- Entsprechend der Sicherheitsanforderung „Das Ortungssystem muss sicherstellen, dass keine falschen oder fehlerhaften Positionsinformationen an ein übergeordnetes System übergeben werden.“ sind die Aktualität der Karte und die Auswertung der Daten kontinuierlich zu überprüfen. Unter der Annahme, dass die Software der digitalen Streckenkarte stabil bleibt, ist zu gewährleisten, dass die Streckenkarte auch nach baulichen Veränderungen im Feld noch aktuell ist. Die Berechnung der Sensordaten sollte entsprechend geeignet redundant ausgelegt werden und erst nach einem Plausibilitätsabgleich mit anderen Positionsdaten als sichere Positionsinformation einem übergeordneten System zugeleitet werden.

Häufigkeit des Auftretens der Gefährdung:

- Entsprechend der Bilder 6.11 und 6.12 nach [EN 50126] – Häufigkeit von Gefährdungsfällen – kann für die Risikoeinschätzung eine Häufigkeit der Kategorie „unwahrscheinlich“ angenommen werden. Das Auftreten der Gefährdung ist unter den o.a. Bedingungen zwar noch möglich, aber unwahrscheinlich. Es wird angenommen, dass die Gefährdung nur in Ausnahmefällen auftritt. Eine quantitative Einschätzung der Häufigkeit ist von der Anwendung abhängig.

Schweregrad und Konsequenzen des Auftretens:

- Entsprechend der Bilder 6.11 und 6.12 nach [EN 50126] – Konsequenzen und Gefährdungsstufen – kann für die Risikoeinschätzung unter Berücksichtigung des Betriebsprozesses eine Gefährdungsstufe von „kritisch“ angenommen werden. Bei einer Kollision sind ggf. ein einzelner Unfalltoter und/oder Schwerverletzte sowie Umweltschäden nicht auszuschließen.

Herausgearbeitete FMEA Nr. 2-1.3
Keine oder fehlerhafte Sensordaten- und Informationsfusion
(FMEA Nr. 1-3.2 als Ursache bereits enthalten):

Risikoeinschätzung:

- Basierend auf potenziell fehlerhaften Daten aus dem GNSS-Modul als GNSS-Position könnte eine falsche Zugposition bei der Sensordaten- und Informationsfusion generiert werden. Sofern keine GNSS-Daten verfügbar sind, sollte eine Abdeckung über andere Sensoren redundant gewährleistet sein.

Maßnahmen:

- Entsprechend der Sicherheitsanforderung „Das Ortungssystem muss sicherstellen, dass keine falschen oder fehlerhaften Positionsinformationen an ein übergeordnetes System übergeben werden." sollten hochverfügbare und sichere Komponenten redundant im System verwendet werden. Die Berechnung der Sensordaten sollte entsprechend geeignet redundant ausgelegt und erst nach einem Plausibilitätsabgleich mit anderen Positionsdaten als sichere Positionsinformation einem übergeordneten System bereitgestellt werden.

Häufigkeit des Auftretens der Gefährdung:

- Entsprechend der Bilder 6.11 und 6.12 nach [EN 50126] – Häufigkeit von Gefährdungsfällen – kann für die Risikoeinschätzung eine Häufigkeit der Kategorie „selten" angenommen werden. Die Gefährdung kann während des Lebenszyklus´ unter den o.a. Bedingungen manchmal auftreten.

Schweregrad und Konsequenzen des Auftretens:

- Entsprechend der Bilder 6.11 und 6.12 nach [EN 50126] – Konsequenzen und Gefährdungsstufen – kann für die Risikoeinschätzung unter Berücksichtigung des Betriebsprozesses eine Gefährdungsstufe von „kritisch" angenommen werden. Bei einer Kollision sind ggf. ein einzelner Unfalltoter und/oder Schwerverletzte sowie Umweltschäden nicht auszuschließen.

Aufgrund der Synonymität der Ergebnisse der prozessbezogenen zweiten FMEA-Betrachtungsstufe und der Eingrenzung nach der RPZ-Risikomatrix werden nachfolgend auf Basis der normativen Vorgehensweise die Betrachtungen der Auftretenswahrscheinlichkeit der Fehlerursache als prozessbezogene Häufigkeit der Gefährdungsfälle sowie die Bedeutung der Fehlerfolge als Gefährdungsstufe bewertet. In der nachfolgenden Matrix sind die relevanten Risikoabschätzungen zur vorbereitenden Risikoeinstufung bzw. -bewertung aufgetragen. Als mögliche Risikoreduktion wurde bereits die in der Risikoprioritätszahl enthaltene Entdeckungswahrscheinlichkeit der Teilsystemfehler berücksichtigt.

Die Einstufungen der aus der FMECA im Folgenden nicht weiter betrachteten Teilsysteme sind in Bild 6.11 in Klammern eingefügt, da diese Werte unterhalb des definierten Grenzrisikos liegen. Die bereits als Fehlerursache analysierten Funktionen der FEMCA (Nr. 1-4.1 und 1-3.2) sind ebenfalls

im Bild eingefügt, werden aber im Folgenden als bereits in der übergeordneten FMECA berücksichtigte Fehlfunktionen betrachtet, sodass in der Risikoabschätzung und -bewertung lediglich die in der zweiten Betrachtungsstufe über dem Grenzrisiko liegenden Werte tiefergehend untersucht werden.

	Angewandte Risikomatrix mit RPZ										
	Auftretenswahrscheinlichkeit der Fehlerursache										
10	sehr häufig										
9	häufig										
8	sehr wahrscheinlich										
7	wahrscheinlich										
6	gelegentlich										
5	selten	(1-1.1; 1-2.1; 1-3.1; 2-1.1)									
4	unwahrscheinlich					(1-4.2)			2-1.3 Fehlerhafte Sensordatenfusion		
3	möglich										
2	relativ unvorstellbar								2-1.2 Fehlerhafte Sensordatenfusion 1-4.1 Datenauswertung GNSS-Position		
1	absolut unvorstellbar								1-3.2 Datenauswertung Map-Matching		
		absolut unbedeutend	unbedeutend	leicht	leicht marginal	marginal	marginal kritisch	kritisch marginal	kritisch	sehr kritisch	katastrophal
		1	2	3	4	5	6	7	8	9	10
				Bedeutung der Fehlerfolge aus Anwendersicht							
	FMECA Risikoeinstufung										
	Tolerierbare Risikogrenze = RPZ 50										

Bild 6.11: FMECA-Risikoeinstufung in der RPZ-Risikomatrix

6.1.8 Angewandte Risikobewertung

Auf normativer Grundlage sowie entsprechend der methodischen Vorarbeiten aus Kapitel 5 mit einer geringfügigen Verschiebung der Grenze zwischen „tolerabel“ und „unerwünscht“ werden in Bild 6.12 die potenziellen und für die weitere Betrachtung relevanten Fehlfunktionen des Ortungssystems in die RPZ-Risikomatrix eingestuft und normativ abgegrenzt. Somit lassen sich die Aussagen treffen, dass die Risiken im ersten Fall (FMEA Nr. 2-1.2: Keine oder fehlerhafte Sensordaten- und Informationsfusion) als „tolerabel“, im zweiten Fall (FMEA Nr. 2-1.3: Keine oder fehlerhafte Sensordaten- und Informationsfusion) als „unerwünscht“ bewertet sind, was gegen die quantitative Aussage der FMECA zu plausibilisieren ist.

Risikomatrix mit RPZ										
Auftretenswahrscheinlichkeit der Fehlerursache										
sehr häufig	unerwünscht				unerwünscht	intolerabel				intolerabel
häufig	tolerabel									
sehr wahrscheinlich				unerwünscht						
wahrscheinlich			tolerabel					intolerabel		
gelegentlich	tolerabel					unerwünscht		unerwünscht		intolerabel
selten	vernachlässigbar				tolerabel					unerwünscht
unwahrscheinlich								**FMECA 2-1.3**		
möglich		tolerabel					tolerabel			
relativ unvorstellbar		vernachlässigbar	tolerabel		tolerabel			**FMECA 2-1.2**		unerwünscht
absolut unvorstellbar	vernachlässigbar				vernachlässigbar	tolerabel			tolerabel	
	absolut unbedeutend	unbedeutend	leicht	leicht marginal	marginal	marginal kritisch	kritisch marginal	kritisch	sehr kritisch	katastrophal
	1	2	3	4	5	6	7	8	9	10
			Bedeutung der Fehlerfolge aus Anwendersicht							

Bild 6.12: Risikobewertung in RPZ-Risikomatrix

Aufgrund des bereits in Kapitel 5 vorgestellten methodischen Vorgehens sind geeignete risikoreduzierende Maßnahmen zu ergreifen, um einerseits qualitativ in der Risikomatrix mit sämtlichen Funktionen mindestens den tolerierbaren Bereich zu erlangen, ergänzend dazu muss auch quantitativ der Wert unterhalb des Grenzrisikos gebracht werden.

Geeignete Maßnahmen sind entsprechend bei der Umsetzung des Systems zu ergreifen, wobei im ersten Fall (FMEA 2-1.2) eine Überwachung der Aktualität der Streckenkarte mit Zustimmung des Eisenbahnunternehmens ausreichend wäre; im zweiten Fall (FMEA 2-1.3) sollte eine technische Risikoreduzierung angestrebt werden. Durch die Auftragung der Ergebnisse in der Risikoskala (Bild 6.13) wird dieser Sachverhalt verdeutlicht. In Anlehnung an Bild 5.12 sind in Bild 6.13 die aus der FMECA abgeleiteten und risikobewerteten Prioritäten mit den entsprechenden Nummerierungen (1-1.1 ff.) in der Risikoskala aufgeführt.

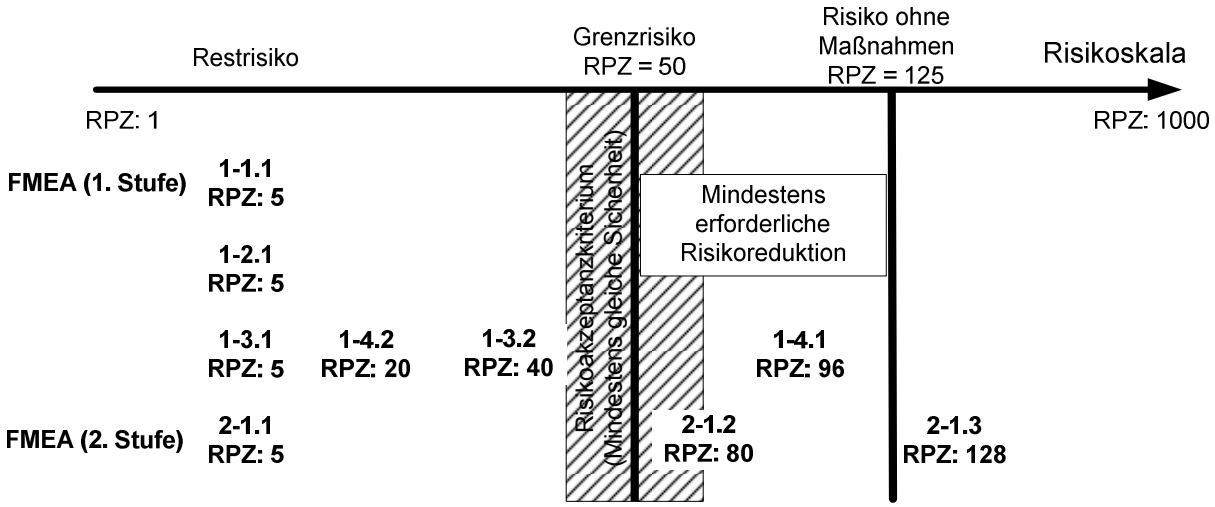

Bild 6.13: Prozessbezogene spezifische erste Risikobewertung für das Ortungssystem

Das betrachtete Grenzrisiko ist in der vorgestellten semiquantitativen Form nach der Risikoeinstufung ermittelt worden. Ergänzend zum Einsatz der FMECA könnten Fehler- bzw. Störungsbaumanalysen nach [IEC 61025] oder auch petrinetzbasierte Analysen nach [IEC 62551] zur quantitativen Bewertung herangezogen werden, in denen die Ausfallraten der Teilsysteme bzw. Systemkomponenten auf das Gesamtsystem Berücksichtigung fänden. Bei neuen Systemen sollte der Testeinsatz eines Prototypensystems zur Generierung von Daten berücksichtigt werden, wodurch Rückschlüsse auf die Ausfallraten der Teilsysteme gezogen werden können. Aufgrund dieser fehlenden Informationsquelle bleibt an dieser Stelle die tiefer gehende quantitative Analyse unberücksichtigt; die Diskussion zum Umgang mit ermittelten Werten oberhalb des Grenzrisikos wird im Folgenden fortgesetzt.

6.1.9 Risikoakzeptanz und -reduktion

Als Risikoakzeptanzkriterium wird bei dieser exemplarischen Sicherheitsuntersuchung der fahrzeugautarken Ortung der „Nachweis mindestens gleicher Sicherheit“ nach [EBO 2008] zugrunde gelegt, welches mit dem in Frankreich gebräuchlichen Risikoakzeptanzkriterium, dem GAMAB-Prinzip (Globalement Au Moin Aussi Bon = insgesamt mindestens genauso gut) nach [EN 50126], vergleichbar ist. Das neue fahrzeugautarke Ortungssystem ist daher einem bereits im Betrieb befindlichen bezüglich der mindestens gleichen definierten Sicherheit gegenüberzustellen. Als Betriebsprozess wird der Zugleitbetrieb herangezogen, der beim Nachweis als Referenzprozess fungiert.

Bei der Referenzuntersuchung sind, wie in Abschnitt 6.1.4 erläutert, im Betriebsprozess zwei verschiedene Betrachtungen des Ortungssystems herausgestellt worden. Einerseits wurde das Ortungssystem als zusätzliche sichere Zugpositionsinformation im herkömmlichen Betriebsprozess in Form des „Rucksacksystems“ vorangestellt, andererseits wurde es sicherheitsrelevant in den Betriebsprozess integriert und ersetzt die herkömmliche Form der Zugpositionsinformation.

Um einen Nachweis der mindestens gleichen Sicherheit zu führen, müssten an dieser Stelle die Statistiken über Kollisionen zwischen Zügen im Zugleitbetrieb auf einer Referenzstrecke ausgewertet werden. Bezogen auf dieselbe Referenzstrecke wären dann unter Berücksichtigung des neuen Systems die potenziellen Gefährdungen entsprechend quantitativ zu bewerten (z.B. durch ermittelte Werte eines Prototyptests) und wie folgt zu vergleichen:

$$\textit{Sicherheit (neues System)} \geq \textit{Sicherheit (herkömmliches System).}$$

Exemplarischer Nachweis durch Risikoreduktion:

Die Forderung „keine oder fehlerhafte Sensordaten- und Informationsfusion“ lässt sich für den Betrachtungsfall FMEA Nr. 2-1.2 durch einen Prozess der kontinuierlichen Aktualitätshaltung der Streckenkarte inkl. Prüfung eine Risikoreduktion erreichen. Die Berechnung der Sensordaten sollte redundant erfolgen.

Für dieselbe Forderung lässt sich im Betrachtungsfall FMEA Nr. 2-1.3 das Risiko durch eine redundante Auslegung der technischen Sicherungsfunktionen mit entsprechender Ausfallüberwachung reduzieren, wodurch die Sicherheit erhöht wird.

Die übergeordneten FMEA der 1. Betrachtungsstufe sind bereits in die o.g. Betrachtungsfälle integriert und bedürfen keiner gesonderten Beachtung der Risikoreduktion.

Unter Einbeziehung der Risikoreduktionen beider Betrachtungsfälle ist eine erneute Berechnung der Risikoprioritätszahl in einer FMECA durchzuführen, um nachzuweisen, dass das Grenzrisiko nach der Systemoptimierung unterschritten wird. Bild 6.14 zeigt die erneute Durchführung der FMECA in der relevanten zweiten Betrachtungsstufe unter Berücksichtigung der diskutierten Risikoreduktionsmaßnahmen.

	Fehlermöglichkeits- und -einflussanalyse (FMEA)								
	Konstr.-FMEA	Prozess-FMEA X	System-FMEA					Gesamtsystem	
	Bestätigung durch betroffene Stellen	Kurzzeichen Teilnehmer		Projektleiter gesehen				Sicherheitsrelevantes Ortungssystem nach DemoOrt	
Systeme/Merkmale	Potentielle Fehler	Potentielle Fehlerfolgen	Potentielle Fehlerursachen	DERZEITIGER ZUSTAND					Empfohlene Maßnahme
				Getroffene Maßnahmen Risikoreduktion	A	B	E	RPZ	
2-1.2 Sensordaten- und Informationsfusion FMECA nach Maßnahmen-umsetzung	Keine oder fehlerhafte Sensordaten und Informations-fusion	Ausfall sichere Positionsinformation (potenzielle Kollision)	Fehlerhafte Daten Map-Matching (mit Weichen-identifikation)	Die Aktualität der Karte und die Auswertung werden kontinuierlich geprüft. Berechnung der Sensordaten sind redundant ausgelegt und werden erst nach Abgleich als sichere Positionsinformation gesendet.	1	8	4	32	
2-1.3 Sensordaten- und Informationsfusion FMECA nach Maßnahmen-umsetzung	Keine oder fehlerhafte Sensordaten und Informations-fusion	Ausfall sichere Positionsinformation (potenzielle Kollision)	Keine oder fehlerhafte Daten GNSS-Position	Hochverfügbare und sichere Komponenten werden im System verwendet. Berechnung der Sensordaten sind redundant ausgelegt und werden erst nach Abgleich als sichere Positionsinformation gesendet.	2	8	3	48	

Bild 6.14: FME(C)A mit Berücksichtigung der Risikoreduktion

Für den Betrachtungsfall 2-1.2 kann durch die kontinuierliche Aktualisierung der Streckenkarte in Verbindung mit der redundanten Auslegung der Sensordatenberechnung, die Auftretenswahrscheinlichkeit *A* exemplarisch halbiert werden. Ebenso kann die Entdeckungswahrscheinlichkeit *E* erhöht werden, da sich ein potenzieller Ausfall im sicheren Zustand über eine längere Zeit offenbart.

Im zweiten Fall 2-1.3 wird eine redundante Auslegung der technischen Sicherungsfunktionen mit entsprechender Ausfallüberwachung berücksichtigt, wodurch in Verbindung mit der Forderung nach hochverfügbaren und sicheren Komponenten Auftretens- und ebenfalls reduziert werden konnten.

Auf diesen Annahmen wurden die RPZ exemplarisch neu ermittelt, wodurch eine Verschiebung der Werte in den tolerierbaren Bereich (Bild 6.15) sowie unterhalb des Grenzrisikos (Bild 6.16) ersichtlich wird. Bild 6.15 stellt diesen Sachverhalt durch Auftragung in der RPZ-Risikomatrix dar.

Risikomatrix mit RPZ

Auftretenswahrscheinlichkeit der Fehlerursache

sehr häufig		unerwünscht			unerwünscht	intolerabel				intolerabel
häufig	tolerabel									
sehr wahrscheinlich				unerwünscht						
wahrscheinlich			tolerabel					intolerabel		
gelegentlich	tolerabel					unerwünscht		unerwünscht		intolerabel
selten	vernachlässigbar				tolerabel					unerwünscht
unwahrscheinlich										
möglich		tolerabel					tolerabel			
relativ unvorstellbar		vernachlässigbar	tolerabel		tolerabel			FMECA 2-1.3		unerwünscht
absolut unvorstellbar	vernachlässigbar				vernachlässigbar	tolerabel		FMECA 2-1.2	tolerabel	
	absolut unbedeutend	unbedeutend	leicht	leicht marginal	marginal	marginal kritisch	kritisch marginal	kritisch	sehr kritisch	katastrophal
	1	2	3	4	5	6	7	8	9	10

Bedeutung der Fehlerfolge aus Anwendersicht

Bild 6.15: RPZ-Risikomatrix – Einordnung nach risikoreduzierenden Maßnahmen

Zur Einordnung der semiquantitativen Ergebnisse nach der Risikoreduktionsdiskussion bietet sich die Darstellung der Risikoskala an (Bild 6.16).

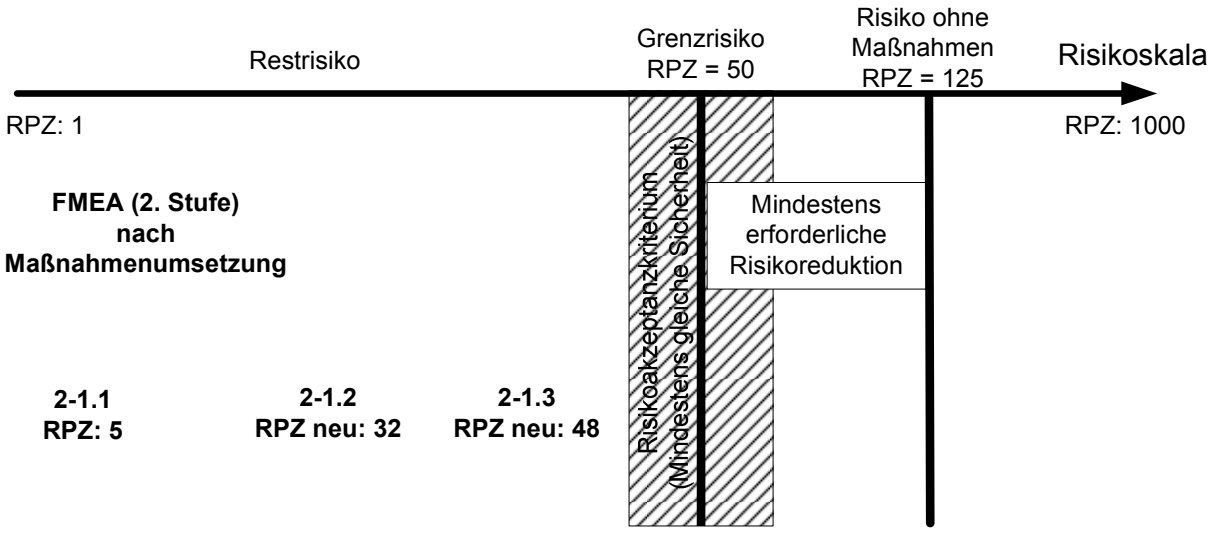

Bild 6.16: Risikoskala nach Risikoreduktionsmaßnahmen

Der Nachweis der mindestens gleichen Sicherheit wäre bereits an dieser Stelle erzielt.

Darüber hinaus kann eine Betrachtung der Systemzuverlässigkeiten die Aussagekraft des Nachweises stärken. Beim ersten Systemfall dem „Rucksacksystem“, wird die zusätzliche sichere Zugpositionsinformation des Ortungssystems den Akteuren des Prozesses als Entscheidungshilfe zur Verfügung gestellt, wodurch die menschliche Zuverlässigkeit der Akteure berücksichtigt werden muss, da sich im Laufe der Zeit ein Vertrauen in das Ortungssystem einstellen wird [Schröder 2009].

Zur tiefergehenden Quantifizierung kann mit entsprechenden Zahlenwerten die Ausfallrate für das Ortungssystem für einen unerkannten gefährlichen Systemausfall unter Berücksichtigung des Ausfalls von Eisenbahnfahrzeugführer (Ef) und Zugleiter (ZL) herangezogen werden.

Daraus lassen sich Bewertungsansätze ableiten, um folgenden Nachweis zu erbringen:

Ausfallrate Zugpositionsinformation < Ausfallrate Personale im Störungsfall

Im zweiten Systemfall wird die fernmündliche Kommunikation zwischen Ef und ZL komplett technisch abgelöst. In diesem Fall ändert sich das Betriebsverfahren geringfügig, die betrieblichen und sicherheitsrelevanten Funktionen bleiben hingegen unverändert. Es entfällt hierbei die Kontrollfunktion durch den Ef sowohl bei der Zugpositionsermittlung als auch bei dem Informationsabgleich nach einer Fahrerlaubnis. Quantitativ gegenübergestellt und ausgewertet werden muss an dieser Stelle entsprechend das Ausfallverhalten des Ef bei Positionsermittlungen und -übertragungen (Meldungen), welches zu Kollisionen zwischen Zügen geführt hat (z. B. aus Unfallstatistiken), mit der Ausfallrate des Ortungssystems für einen unerkannten gefährlichen Systemausfall, der zu einer Kollision führen könnte. Zur Erbringung des Nachweises lassen sich auch in diesem Fall daraus Bewertungsansätze ableiten:

Ausfallrate Zugpositionsinformation < Ausfallrate Ef

Im Vergleich sind im ersten Fall zwar die Betriebspersonale (Ef und ZL) in Summe zu betrachten, bei ihrer Tätigkeit aber nur auf den Störungsfall des ergänzenden Ortungssystems zeitlich diskret zu bewerten. Die Ausfallrate der Zugpositionsinformation muss im zweiten Fall wesentlich kleiner ausfallen, da hier die Ausfallrate des Ef mit diskreter Tätigkeitsausübung einer kontinuierlichen Tätigkeit gegenübergestellt werden muss.

Insgesamt ist bei beiden Gegenüberstellungen erkennbar, dass die Ausfallraten des Ortungssystems stets kleiner als die des zu vergleichenden menschlichen Systems sein müssen, was aufgrund der multisensorischen Umsetzung des technischen Systems im Bereich mehrerer 10er Potenzen möglich ist. Zur weiteren Risikoreduktion entsprechend der jeweiligen Sicherheitsphilosophie des betreibenden Unternehmens sollte das Ortungssystem mit Ausfalldetektoren zur Diagnose ausgestattet werden, welche einen Systemausfall zuverlässig erkennen lassen.

Aufgrund des Fehlens geeigneter Zahlenwerke muss auf eine tiefer gehende quantitative Betrachtung an dieser Stelle verzichtet werden. Vergleichbar kann der „Nachweis mindestens gleicher Sicherheit“ bei verfügbaren Zahlenwerken für alle betrieblichen Referenzsysteme und Prozesse umgesetzt werden.

Eine abschließende Bewertung und Einordnung der Sicherheit für die betrachteten exemplarischen Anwendungsfälle – unter Berücksichtigung der Verfügbarkeit – wird in der abschließenden Sicherheitsbewertung in Abschnitt 6.3 gegeben.

6.2 Exemplarische Verfügbarkeitsanalyse

Als methodische Ergänzung zur Sicherheitsuntersuchung ist die Systemverfügbarkeit für das fahrzeugautarke Ortungssystem zu betrachten, da das System neben den Sicherheitsaspekten auch verfügbarkeitsrelevant eingesetzt werden muss, um ein zukunftsfähiges Eisenbahnsystem innovativ zu unterstützen. Die Systemverfügbarkeit kann ebenfalls risikoreduzierend Einfluss nehmen, weshalb in der abschließenden Sicherheitsbewertung methodisch die Sicherheit der Verfügbarkeit gegenübergestellt wird.

Bei der folgenden Analyse werden erneut die in Abschnitt 6.1.3 erläuterten, zwei verschiedenen Sichten des Ortungssystems im Betriebsprozess aufgegriffen und als Fälle 1 und 2 bezeichnet.

Die *MUT* (mean up time), als mittlere Zeit zwischen zwei sicherheitsrelevanten Ausfällen, stellt sich für das fahrzeugautarke Ortungssystem im herkömmlichen Betriebsprozess des Zugleitbetriebs als Zeit zwischen zwei Fehlhandlungen des Betriebspersonals dar. Falsche, fehlerbehaftete, unzeitige oder fehlende Zugschlussmeldungen sowie Fahrtaufträge kommen in der Praxis vor, führen aber auf Nebenbahnen nur selten zu Unfällen aufgrund der Plausibilisierung durch redundant wirkendes Personal und der geringen Betriebsleistungsdichte. (Eine Unfallstatistik für belastbarere Aussagen durch die Deutsche Bahn AG war bei der Literaturrecherche zu dieser Arbeit nicht zu erhalten).

Für die *MDT* (mean down time), als mittlere Zeit, in der das System nach erkanntem und damit sicherem Ausfall nicht zur Verfügung steht (Unverfügbarkeit), muss die Zeit angenommen werden, in der das Betriebspersonal nicht zur Verfügung steht, um Zugpositionsinformationen zu übermitteln oder zu empfangen. Diese Zeit kann als sehr klein angenommen werden, da sich nur personelle Totalausfälle (fehlen des Personals) entscheidend auf die *MDT* auswirken würden [FMEA 2006].

Würde beispielhaft alle 100 Tage (*MUT* = 100 Tage) das Betriebspersonal bezogen auf das fernmündliche Ortungssystem einen sicherheitsrelevanten Ausfall verursachen [Hinzen 1993] und es tritt statistisch alle 5 Jahre (*MDT* = 1 / 1.825 Tage) der Fall auf, dass das Personal einen kompletten Tag total ausfällt (nicht zur Verfügung steht) und somit das System unverfügbar wird, lässt sich eine exemplarische Systemverfügbarkeit von $A = 0{,}9999945$ (nach Formel 4.2) errechnen, die es durch ein innovatives Ortungssystem mindestens zu erreichen gilt.

Genauere Zahlenwerte für eine detaillierte Auswertung wären betreiberseitigen Statistiken zu entnehmen bzw. in Testphasen und Systemerprobungen zu ermitteln.

Im o.a. 1. Fall, bei dem das Ortungssystem als „Rucksacksystem“ dem herkömmlichen Betriebsprozess zur Verfügung gestellt wird, kann die *MUT* erhöht werden, wenn das Betriebspersonal vor sicherheitsrelevanten Fehlern eine Möglichkeit zur Plausibilisierung hat. Aufgrund der Zusätzlichkeit des technischen Ortungssystems ändert sich die *MDT* nahezu nicht, vorausgesetzt, dass das technische System über eine sichere und zuverlässige Ausfallerkennung verfügt. Aufgrund der Systemauslegung mit Redundanz von Technik und Personal wird exemplarisch eine *MUT* von 10

Jahren (3.650 Tage) als untere Grenze angenommen. Für die *MDT* wird festgelegt, dass entsprechend alle 10 Jahre das System für einen Tag (24 Std.) nicht zur Verfügung steht (*MDT* = 1 / 3.650). Somit errechnet sich für den 1. Fall eine beispielhafte Systemverfügbarkeit von *A* = 0,9999999 (Formel 4.2).

Im o.a. 2. Fall, bei dem das Ortungssystem sicherheitsrelevant in den Betriebsprozess integriert wird und die herkömmliche Form der Zugpositionsinformation ersetzt, entfallen einseitig gerichtete, fernmündlich übertragene Zugpositionsmeldungen durch den Eisenbahnfahrzeugführer. Die *MUT* verringert sich aufgrund fehlender Redundanz des Personals leicht, wobei hier auch die Kommunikationsverfügbarkeit eines Funksystems o.ä. noch mit zu berücksichtigen ist, welche die *MUT* ergänzend leicht reduziert. Unter der beispielhaften Annahme, dass sich die *MUT* durch die technische Unterstützung lediglich um den Faktor 3 gegenüber dem reinen Zugleitbetriebsverfahren erhöht, wird für den 2. Fall eine exemplarische Verfügbarkeit von *A* = 0,9999991 erreicht.

Eine Gegenüberstellung der exemplarischen Verfügbarkeiten zeigt zusammenfassend Bild 6.17.

Ortung im Betriebsprozess	***MUT* – mean up time (getroffene Annahme)**	***MDT* – mean down time (getroffene Annahme)**	***A* – exemplarisch errechnete Verfügbarkeit**
Fernmündliche Zugpositionsinformation im herkömmlichen Zugleitbetrieb.	100 Tage	1 Tag innerhalb von 5 Jahren (*MDT* = 0,0005479 Tage)	*A* = 0,9999945
1. Betrachtungsfall: Innovatives Ortungssystem stellt zusätzliche sichere Zugpositionsinformation im herkömmlichen Zugleitbetrieb bereit.	3.650 Tage (10 Jahre)	1 Tag innerhalb von 10 Jahren (*MDT* = 0,000274 Tage)	*A* = 0,9999999
2. Betrachtungsfall: Innovatives Ortungssystem wird sicherheitsrelevant in den Betriebsprozess integriert und ersetzt die herkömmliche Form der Zugpositionsinformation.	300 Tage	1 Tag innerhalb von 5 Jahren (*MDT* = 0,0005479 Tage)	*A* = 0,9999991

Bild 6.17: Zusammenfassung der Verfügbarkeitsberechnung

Durch regelmäßige Wartung bzw. Instandhaltung des technischen Systems können die Werte maßgeblich beeinflusst und die Gesamtsystemverfügbarkeiten weiter erhöht werden.

6.3 Sicherheitsbewertung

Zur abschließenden Validation der Sicherheitsuntersuchung wird unter Berücksichtigung der RAMS-Kriterien eine Bewertung der Sicherheit gegeben. Mit Hilfe der Gegenüberstellung von Sicherheit und Verfügbarkeit soll eine grafische Einordnung zum Nachweis der gleichen Sicherheit gegeben werden.

Bild 6.18 spiegelt die integrierte, semiquantitative und transparente Einordnung der Ortung im aktuellen Betriebsprozess des Zugleitbetriebes (1) exemplarisch im Sicherheits-Verfügbarkeits-diagramm wider, dessen Achsen logarithmisch skaliert sind. Durch Anwendung einer erneuten FMECA sowie der Umwandlung in die Risikomatrix kann im günstigsten Fall eine RPZ von 50 ermittelt werden. Da das System inkl. der betrieblichen Prozesse in Betrieb ist und aufgrund einer Vielzahl von Regeln relativ sicher funktioniert, kann der Grenzwert RPZ = 50 zur weiteren Betrachtung angenommen werden.

Ergänzend ist rein qualitativ zur referenzierenden Einordnung auch das Standard- bzw. Zugmeldeverfahren (2 und 3) mit unterschiedlichen Ortungssystemen integriert. Beide Ortungs-systeme sind allein nur als bedingt sicher anzusehen. Aufgrund der übergeordneten und komplexen Stellwerkstechnik werden die Systeme sicherheitsrelevant.

Die Anordnung des Zugmeldeverfahrens im Bereich des sicheren Systembetriebes bei höherer Sicherheit und Verfügbarkeit gegenüber dem Zugleitbetrieb (1) wurde aufgrund der technisch basierten Systemlösung umgesetzt.

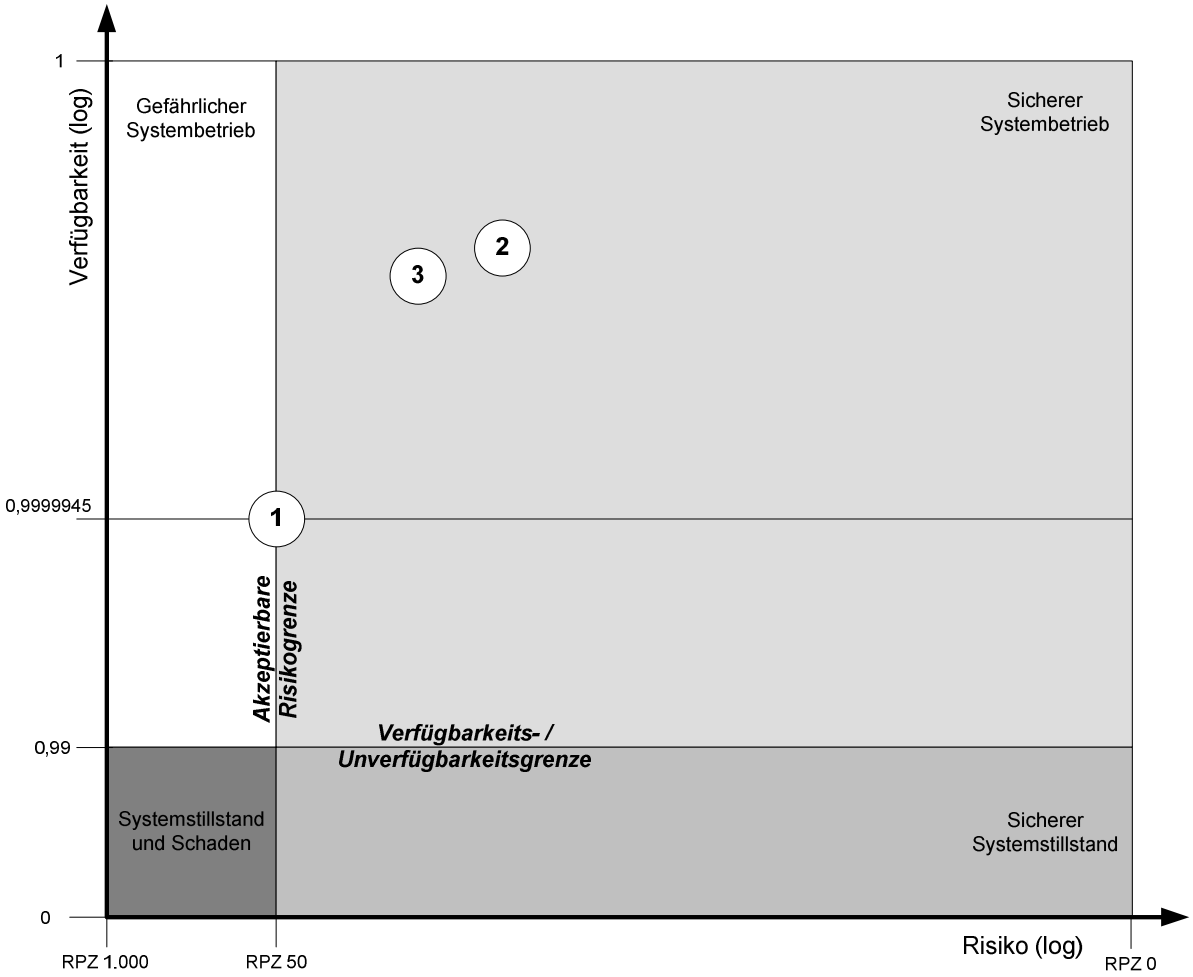

Bild 6.18: Ortung im Vergleich unter Sicherheits- und Verfügbarkeitsaspekten

Die Nummerierung stellt sich wie folgt dar:

① Zugleitbetrieb mit fernmündlicher Zugschlussmeldung als Ortung

Aufgrund der Umsetzung der Regeln durch das Personal im ZLB ist die Einordnung im „sicheren Systembetrieb“ möglich. Die Verfügbarkeit wurde den Annahmen aus Bild 6.18 entnommen.

② Standard- bzw. Zugmeldeverfahren mit Ortung mittels Achszählern

Das rein qualitativ eingeordnete Verfahren mit der Achszählerortung ist aufgrund der hohen technischen Ausstattung mit Sicherungsfunktionen und Rückfallebenen deutlich im sicheren Bereich zu finden. Auch die Verfügbarkeit ist höher als beim ZLB angeordnet.

③ Standard- bzw. Zugmeldeverfahren mit Ortung über Gleisstromkreise

Die Zuordnung des Zugmeldeverfahrens mit Gleisstromkreisortung ist aufgrund von Einflüssen durch die Fahrzeuge (z.B. Sandung) etwas weniger verfügbar und dadurch auch unsicherer als die Achszählerortung, was durch die rein qualitative Gegenüberstellung verdeutlicht wird.

Eine Bewertung der exemplarisch ermittelten Größen unter semiquantitativer Integration in das Sicherheits-Verfügbarkeitsdiagramm wird nachfolgend dargestellt. Zur Verdeutlichung stellt

Bild 6.19 das generische Sicherheits-Verfügbarkeitsdiagramm der Ortung dar. Zur Plausibilisierung wird dadurch ersichtlich, dass der Zugleitbetrieb mit fernmündlicher Zugschlussmeldung, welcher in der vorhergehenden Betrachtung mit einer RPZ von 50 berücksichtigt wurde, im verfügbaren Bereich zwischen dem sicheren und gefährlichen Systembetrieb in Form eines „Regelkreises“ wechseln kann, wenn personalgestützt der Zustandsübergang der Fehlererkennung und Korrektur etc. berücksichtigt wird.

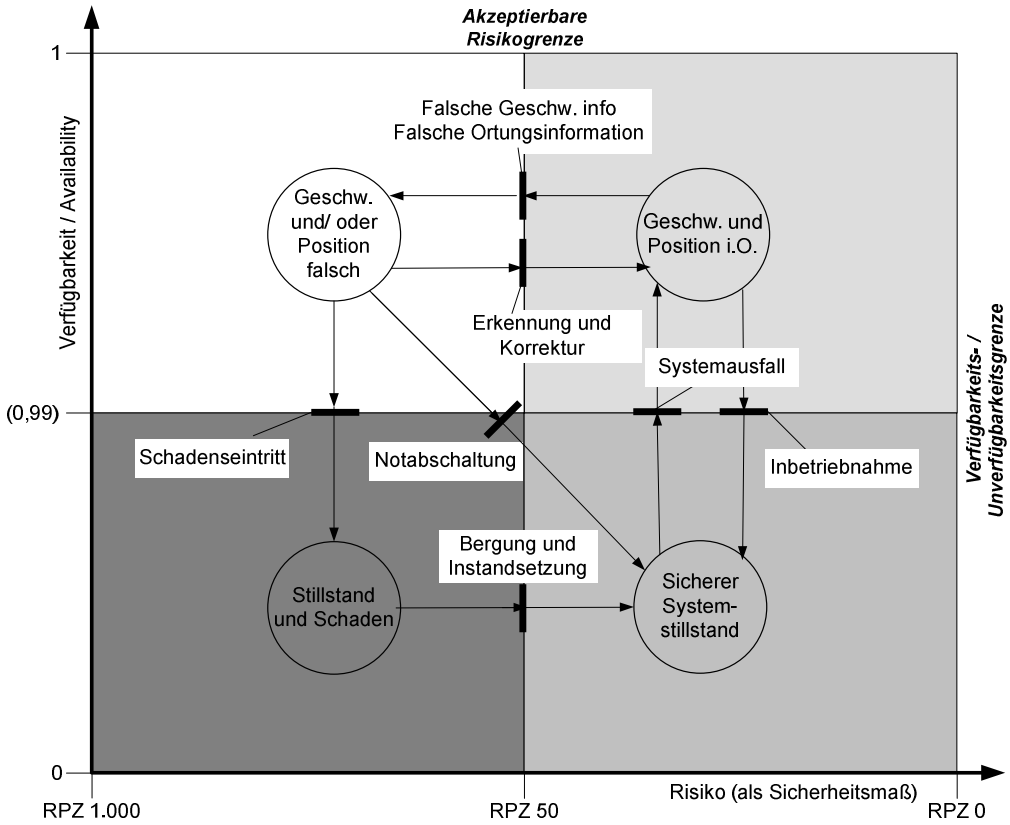

Bild 6.19: Generisches Sicherheits-Verfügbarkeitsdiagramm der Ortung

Bei der abschließenden Bewertung wird die Betrachtung des derzeitigen Zugleitbetriebs auf Nebenbahnen unter Einordnung der Sicherheit und Berücksichtigung der Verfügbarkeitsanalyse aus Bild 6.17 herangezogen.

Mit Ergänzung des fahrzeugautarken Ortungssystems und den Betrachtungen aus den vorhergehenden Abschnitten lässt sich die Einordnung der Systeme im Diagramm verschieben und der Nachweis mindestens gleicher Sicherheit plausibilisieren (Bild 6.20).

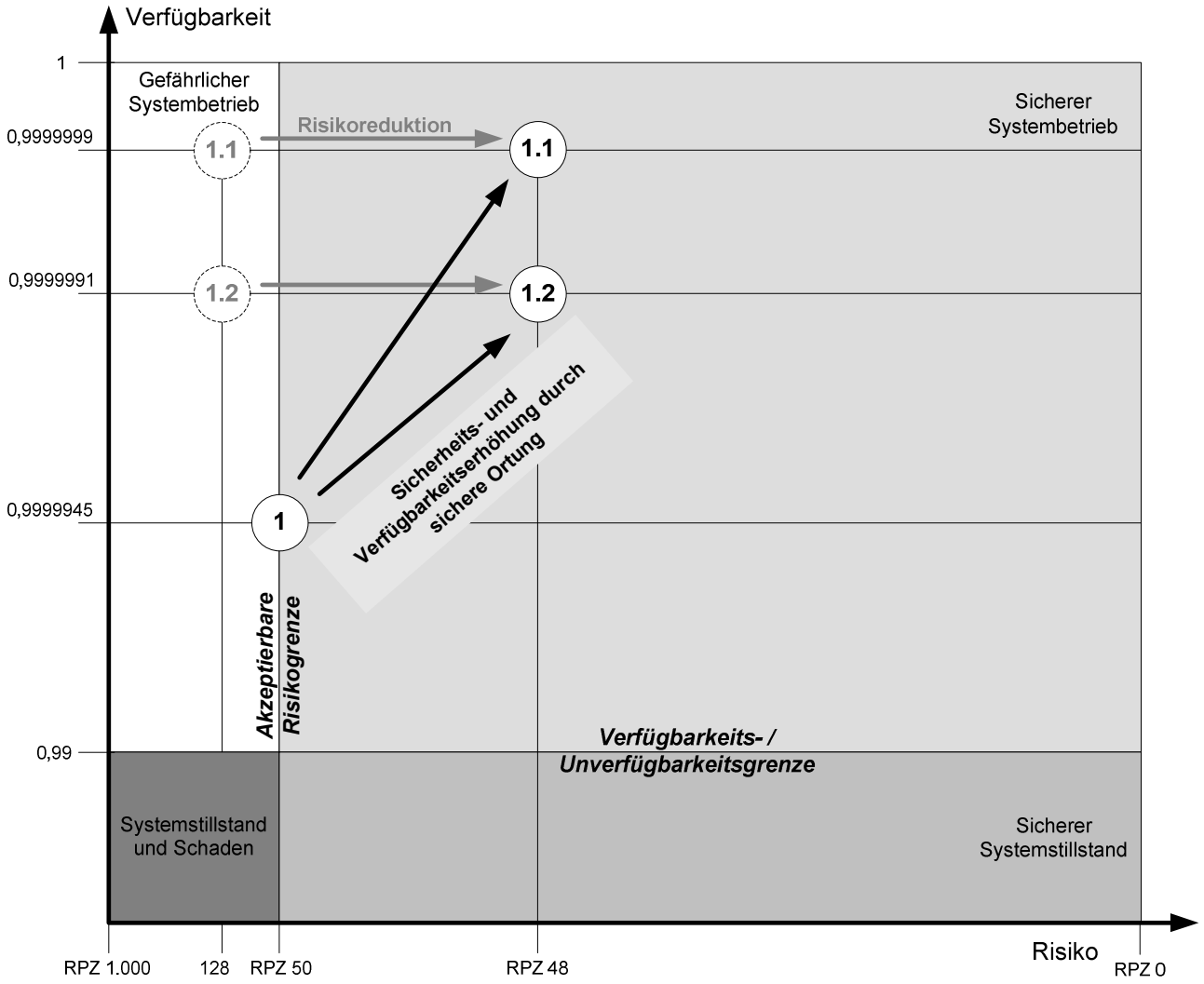

Bild 6.20: Sicherheitsbewertung des Ortungssystems im Sicherheits-Verfügbarkeitsdiagramm

Ersichtlich wird, dass unter Berücksichtigung der in der Sicherheitsuntersuchung semiquantitativ getroffenen Annahmen und der exemplarischen Berechnung der Verfügbarkeit bereits eine positive Tendenz sowohl der Sicherheit, als auch der Verfügbarkeit durch das technische Ortungssystem darstellbar ist.

Die Nummerierung stellt sich wie folgt dar:

① Zugleitbetrieb mit fernmündlicher Zugschlussmeldung als Ortung

①.① Zugleitbetrieb mit fernmündlicher Zugschlussmeldung als Ortung und der zusätzlichen Positionsermittlung durch das sicherheitsrelevante Ortungssystem als „Rucksacksystem“

Durch die reine Ergänzung des Ortungssystems in das Betriebsverfahren wird die Sicherheit erhöht und auch die Verfügbarkeit steigt deutlich.

①.② Zugleitbetrieb mit der Positionsbestimmung durch das sicherheitsrelevante Ortungssystem in einem übergeordneten Sicherungssystem (ohne Kommunikationsausfälle)

Durch den Wegfall der Plausibilisierung der Fahrzeugposition durch den Ef wird die Verfügbarkeit leicht abgesenkt, da ein Ausfall des Ef keine Berücksichtigung in der Systemsicht erfährt, die Sicherheit sinkt ohne Risikoreduktion in den Bereich des „gefährlichen Systembetriebs“. Erst durch geeignete risikoreduzierende Maßnahmen (z.B. durch Integration von Redundanzen) kann die Sicherheit in den Bereich des „sicheren Systembetriebs“ verlagert werden; würde aber, aufgrund der fehlenden Rückfallebene (Ef), auf demselben Niveau wie (1.1) bleiben.

Im Rahmen der RAMS-Parameter blieben bisher Instandhaltung als Schlüssel zwischen Sicherheit und Verfügbarkeit wie auch die Zuverlässigkeit der einzelnen Teile des dekomponierten Systems unberücksichtigt. Durch Ergänzung und quantitative Auslegung der beiden Größen lassen sich Sicherheit durch weitere Risikoreduktion und auch Verfügbarkeit durch kontinuierliche und präventive Instandhaltung des Systems zusätzlich erhöhen.

7 ZUSAMMENFASSUNG UND AUSBLICK

7.1 Zusammenfassung

Aufgrund der aktuell positiven Entwicklung im Schienenverkehrsmarkt stellt sich die Frage nach Innovationen, um die Leistungsfähigkeit der derzeitigen Eisenbahninfrastruktur mit relativem Aufwand kurzfristig und aus wirtschaftlicher Sicht zu erhöhen. Ein Lösungsansatz ist dabei in der fahrzeugautarken Ortung mit Sicherheitsrelevanz zu finden, da aufgrund der gewachsenen Historie in diesem Bereich bis heute ausschließlich auf streckenseitige Komponenten und Personal zurückgegriffen wird, wodurch die Streckenleistungsfähigkeiten beeinträchtigt werden. Die vorliegende Arbeit stellt am Beispiel der innovativen fahrzeugautarken Ortung im Schienenverkehr eine durchgängige, normkonforme und strukturierte Methode für eine qualitative und in Ansätzen semiquantitative Sicherheitsuntersuchung mit praktischer Validation vor.

Ausgehend von der Abstrahierung des Eisenbahnsystems in Kapitel 2 werden Automatisierung und Innovationen im Schienenverkehr allgemein und unter dem technischen Anwendungsbezug betrachtet. Rechtliche Grundlagen für Sicherheitsfragen sowie Fragen der späteren Systemzulassung werden untersucht und für tiefergehende Analysen die Betriebsverfahren als Eisenbahnbetriebs-grundlagen herangezogen.

Die Ortung im Schienenverkehr wird in Kapitel 3 im Einzelnen tiefergehend betrachtet. Dabei wird berücksichtigt, für welche Systembereiche die Ortung relevant ist und wo bei derzeitiger Anwendung Innovationspotenziale erkennbar werden. Erste Lösungsansätze für ein ganzheitliches, sicherheits-relevantes System werden vorgeschlagen und mit ausgewählten Referenzprojekten belegt.

Zur Integration eines innovativen, auf Sicherheit basierenden Ortungssystems in die bestehenden Eisenbahnleitsysteme wird in Kapitel 4 die methodische Auseinandersetzung mit den Eigenschaften der Verlässlichkeit (RAMS) erarbeitet. Dabei werden Beschreibungsmittel vorgestellt und die theoretischen Inhalte einer Sicherheitsanalyse sowie einer Sicherheitsnachweisführung verknüpft. Nach einer Definitionsabgrenzung wird eine Gegenüberstellung von Sicherheit und Verfügbarkeit dargestellt, um das methodische Konzept für eine praktische Anwendung zu erarbeiten. Auf Basis der Grundlagen wird die durchgängige generische Methode einer Sicherheitsuntersuchung umfassend in Kapitel 5 vorgestellt. Zur Validation der Sicherheitsuntersuchung wird anhand der fahrzeugautarken Ortung in Kapitel 6 die Methode exemplarisch angewendet. Die qualitative Untersuchung beinhaltet auch eine semiquantitative Umsetzung, sofern numerische Werte vorhanden waren oder eine geeignete Abschätzung sinnvoll erschien. In Abschnitt 6.3 erfolgte eine abschließende Bewertung der Sicherheit durch Einordnung der Ergebnisse in Größen der Sicherheit und Verfügbarkeit.

Eine durchgängige Methode zur Sicherheitsuntersuchung wurde durch die exemplarische Anwendung bestätigt. Neue Forschungsansätze wurden dabei berücksichtigt und methodisch miteinander verknüpft, so dass eine Grundlage für sicherheitsrelevante Bearbeitungen im Umfeld

der Eisenbahnsicherungstechnik unter Berücksichtigung der fahrzeugautarken Ortung geschaffen wurde. Aufgrund fehlender realer Daten, die durch die Eisenbahnunternehmen nicht umfassend zur Verfügung standen, mussten z.T. exemplarische Annahmen für eine Quantifizierung getroffen werden.

Fragen der Systemabgrenzung, der Funktionsableitung, der Unterscheidung zwischen betrieblichen Funktionen und Sicherheitsfunktionen, der Untersuchungstiefe, der anzuwendenden Richtlinien und Standards, der Sicherheits- und Risikoeinschätzung, des akzeptierbaren Risikos, der Sicherheitskultur des herstellenden und betreibenden Unternehmens sowie der Notwendigkeit der umfassenden Dokumentationen wurden ausführlich beantwortet.

7.2 Ausblick

Die im Rahmen dieser Arbeit vorgestellte durchgängige Methode zur Sicherheitsuntersuchung kann auch in quantitativer Form in der Praxis angewendet werden. Zur vertiefenden Analyse und genaueren Abschätzung des Risikos wären jeweils aktuelle und umfassende Zahlenwerte vorteilhaft. Aufgrund der allgemeingültigen Vorgehensweise ist diese Methode nicht allein auf fahrzeugautarke Ortungssysteme bzw. auf sicherheitsrelevante, elektronische Systeme der Signaltechnik beschränkt, eine Übertragung auch auf andere Bereiche der Automatisierungstechnik mit Sicherheitsrelevanz liegt auf der Hand.

Nach der aktuellen Umstrukturierung der einschlägigen, in dieser Arbeit vorgestellten CENELEC-Normen, werden in der neuen, integrierten „EN 50126“ (vorläufige Bezeichnung) auch andere Bereiche des Bahnsystems, z.B. Fahrzeuge, nach RAMS-Aspekten zu analysieren sein, wozu die Methode ebenfalls insgesamt oder in Auszügen herangezogen werden kann. Die Beherrschung einer einfachen und durchgängigen Methode steht dabei im Vordergrund. Komplexe Beschreibungsmittel und Methoden sind in der Praxis eher ungeliebt und werden daher nur bedingt angewendet. Aufgrund der steigenden Komplexität der Systeme wird der Einsatz quantitativer Methoden zur Untersuchung der Sicherheit zunehmend unumgänglich, weshalb die in dieser Arbeit vorgestellte semiquantitative Methode zur Gesamtsicherheit eines modernen Bahnsystems beitragen kann.

Der in der Fachwelt teilweise schwer nachvollziehbare „Glaskugelblick“ bei quantitativen Risikoanalysen kann durch die semiquantitative Methode kompensiert werden. Ein Restrisiko, welches bei (komplexen) Systemen grundsätzlich besteht, kann durch einen Grenzwert in Form der Risikoprioritätszahl bewertet werden. In der Erweiterung der Methode wären mit Hilfe geeigneter Toolunterstützung durch Simulationen am Prozessmodell die Zusammenlegung der Risikofaktoren A (Auftretenswahrscheinlichkeit) und E (Entdeckungswahrscheinlichkeit) denkbar, um die Risikoprioritätszahl noch präziser zur Bewertung der Sicherheit heranzuziehen. Insgesamt ließen sich Teile der Methode selbst automatisieren und durch ein rechnergestütztes Werkzeug erweitern.

Das vorgestellte System zur sicherheitsrelevanten fahrzeugautarken Ortung auf Basis des DemoORT-Projekts kann kostengünstig realisiert werden und bietet daher eine hervorragende Basis bei zukünftigen Anwendungen für innovative Sicherungseinrichtungen [DemoORT 2007].

Ein offener Punkt bleibt die abschließende Lösung der fahrzeugseitigen Zugintegritätsprüfung, die technisch zwar realisierbar ist, aufgrund der gewünschten Migrationsfähigkeit aber schwierig bleibt. In Verbindung mit einer leistungsfähigen Lösung der Zugintegritätsprüfung würde der vorgestellte technische Ansatz eine geeignete Basis für ETCS im Level 3 darstellen und nachhaltig einen Beitrag zum innovativen Schienenverkehr der Zukunft leisten.

Gleichwohl wird eine absolute Sicherheit ohne Risiko auch im innovativen Schienenverkehr der Zukunft selbst bei maximalem Aufwand wohl kaum erreichbar sein.

LITERATURVERZEICHNIS

[Alcouffe/Barbu 2001] Alcouffe, F.; Barbu, G.: APOLO – Advanced positon locator system. UIC Paris, Projekt-Endbericht, 2001.

[Baier/Enning 2006] Baier, M.; Enning, M.: FlexCargoRail – ein Fahrzeugsystem für effizienten Einzelwagenverkehr. In „Logistik Management“, März 2006.

[Barbu 2008] Barbu, G.: GEORAIL – Railway geodesy Guidelines for use of absolute coordinates in railway geo-reference applications. UIC Paris, 2008.

[Barbu et al. 2008] Barbu, G.: (Hrsg.) GNSS / Galileo certification for rail safety applications. Railway requirements and the strategic position of UIC. UIC Paris, 2008.

[Becker et al. 2005] Becker, U.; Hänsel, F.; May, J.; Poliak, J., Schnieder, E.: Vehicle Autarkic Positioning as a Basis for a Low Cost Train Protection System on Secondary Lines, DemoORT Projektbericht, Technische Universität Braunschweig, 2006.

[Becker/Schnieder 2004] Becker, U.; Schnieder, E.: Requirements and Potentials of Safety Relevant Satellite based Localisation Techniques for Train Control and Protection. Tagungsband “Satellite-based applications for railways”, UIC ERRI, Paris, 2004.

[Berndt et al. 2006] Berndt, T.; Gather, M.; Sommer, S.: Bewertung von Verfahren zur Sicherung von Eisenbahnnebenstrecken. In Signal und Draht, März 2006.

[Bertsche 2004] Bertsche, B.; Lechner, G.: Zuverlässigkeit im Fahrzeug- und Maschinenbau Zuverlässigkeit im Fahrzeug- und Maschinenbau. Ermittlung von Bauteil- und Systemzuverlässigkeiten, 3., überarb. u. erw. Aufl., VDI – Spinger Verlag, 2004.

[Bikker 1998] Bikker, G.; Klinge, K.-A.; Röver, S.; Schroeder, M.; Schnieder, E.: RailOrt – Ortung im spurgebundenen Verkehr auf der Basis von Satelliten-Navigation. ETR – Eisenbahntechnische Rundschau, Februar 1998.

[Böhringer 2008] Böhringer, F.: Gleisselektive Ortung von Schnienenfahrzeugen mit bordautonomer Sensorik. Dissertation, Schriftenreihe des Instituts für Mess- und Regelungstechnik, Universitätsverlag Karlsruhe, 2008.

[Boese 2007] Böse, J. W.: Planungsinstrumente zur Realisierung von Prozessinnovation mit Beispielen aus der Verkehrslogistik; Dissertation – Shaker Verlag, Aachen, 2007.

[Braband 2005] Braband, J.: Risikoanalysen in der Eisenbahn-Automatisierung (Edition SIGNAL+DRAHT); Eurailpress-Verlag, 1. Auflage, 2005.

[Chouikha et al. 2000] Chouikha, M.; Einer, S.; Meyer zu Hörste, M.; Schnieder, E.: Ansätze zur Entwicklung von Eisenbahnleitsystemen auf der Basis von Petrinetzen. In: Schnieder, E., Hrsg.: Forms 2000 – Formale Techniken für die Eisenbahnsicherung; VDI-Fortschrittbericht, Reihe 12, Düsseldorf, 2000.

[Däubler 2002] Däubler, L.; Bikker, G.; Schnieder, E.: SATNAB – Satellitengestütztes Navigations-Bodenexperiment. In Signal+Draht, Juni 2002.

[DemoORT 2007] Beisel, D.; Hänsel, F.; Poliak, J.; May, J.; Becker, U.; Schnieder, E.: DemoOrt – Satellitenbasierte fahrzeugautarke Ortung im Schienenverkehr. In: Gesamtzentrum für Verkehr Braunschweig e. V., Hrsg.: Tagungsband der POSITIONs 2007, Oktober 2007.

[DLR 2009] Deutsches Zentrum für Luft- und Raumfahrt: RCAS-Projekt zur Vermeidung von Kollisionen. Internet Download: Handout Nr. 8 (DLR: 20813 – RCAS.pdf; www.dlr.de/ts), 2009.

[Drewes 2009] Drewes, J.: Verkehrssicherheit im systemischen Kontext. Dissertation, Institut für Verkehrssicherheit und Automatisierungstechnik, Technische Universität Braunschweig, 2009.

[Drewes/May 2007] Drewes, J.; May, J.: Entwicklung strukturierter Gefahrenlisten am Beispielsystem „Stellwerk“. In Signal und Draht, Jan./Febr. 2007.

[Duczek/Braband 2002] Duczek, E., Braband, J.: Die Einführung der CENELEC-Normen – eine Herausforderung für die betriebliche Weiterbildung. In Signal und Draht, April 2002.

[EKA 2003] Schnieder, E., Hrsg.: Tagungsband der 8. Fachtagung „Entwurf komplexer Automatisierungssysteme“; EKA 2003. Institut für Verkehrssicherheit und Automatisierungstechnik, Technische Universität Braunschweig, Juni 2003.

[Ellwanger 2004] Ellwanger, Gunther; Hochgeschwindigkeitsverkehr in Europa wieder auf Erfolgskurs – Verkehrsprognosen 2020; in ETR – Eisenbahntechnische Rundschau, 2004.

[Engelberg 2001] Engelberg, T.: Geschwindigkeitsmessung von Schienenfahrzeugen mit Wirbelstrom-Sensoren. Dissertation, Schriftenreihe des Instituts für Mess- und Regelungstechnik, Universitätsverlag Karlsruhe, 2001.

[Erdmann et al. 1994] Erdmann, L.; Schnieder, E.; Schielke, A.G.: Referenzmodell zur Strukturierung von Leitsystemen. In at – Automatisierungstechnik, 1994.

[Fay 1999] Fay, A.: Wissensbasierte Entscheidungsunterstützung für die Disposition im Schienenverkehr. Dissertation, Technische Universität Braunschweig, VDI-Verlag, Düsseldorf, 1999.

[Filip et al. 2001] Filip, A.; Mocek, H.; Bazant, L.: Zugortung auf GPS/GNSS-Basis für sicherheitskritische Anwendungen. In Signal und Draht, Mai 2001.

[FMEA 2006] FMEA – Fehlermöglichkeits- und Einflussanalyse; Deutsche Gesellschaft für Qualität e.V. DGQ-Band 13-11 (Taschenbuch), 4. Auflage, 2006.

[Galcert 2007] Hänsel, F.; May, J.; Poliak, J.; Becker, U.; Schnieder, E.: Satellite Based Low Cost Train Protection System for Secondary Railways Lines. Proceedings of the International Symposium on Certification of GNSS Systems and Services – Tagung CERGAL, Braunschweig, April 2007.

[Geistler 2006] Geistler A.: Bordautonome Ortung von Schienenfahrzeugen mit Wirbelstrom-Sensoren. Dissertation, Schriftenreihe des Instituts für Mess- und Regelungstechnik, Universitätsverlag Karlsruhe, 2006.

[Geistler/Böhringer 2004] Geistler, A.; Böhringer, F.: Ortung von Schienenfahrzeugen mit bordautonomer Sensorik. In ZEVrail, 11/12 2004, 2004.

[Gericke 2008] Gericke, C.: Technische Lösungen zur fahrzeugseitigen Zugintegritäts-prüfung; Diplomarbeit, Institut für Verkehrssicherheit und Automatisierungstechnik, Technische Universität Braunschweig, 2008.

[Gralla 1999] Gralla, D.: Eisenbahnbremstechnik; Werner Verlag GmbH & Co. KG, Düsseldorf, 1999.

[Gu 2005] Gu, X.: Feasibility of GNSS/Galileo-based train location for safety relevant applications. In Signal und Draht, Jan./Febr. 2005.

[Gutsche 2009] Gutsche, K.: Integrierte Bewertung von Investitions- und Instandhaltungsstrategien für die Bahnsicherungstechnik. Dissertation, Technische Universität Braunschweig, 2009.

[Hauschildt 2007] Hauschildt, J.; Salomo, S.: Innovationsmanagement. 4., überarbeitete, ergänzte und aktualisierte Auflage, Vahlen-Verlag, 2007.

[Hänsel et al. 2006] Hänsel, F.; Lux, M.; May, J.; Poliak, J.; Becker, U.; Schnieder, E.: Reference Measurement Platforms for Satellite Based Safety Applications. Tagungsband "International Symposium on Operational Space Applications", Toulouse (F), 2006.

[Hänsel et al. 2007] Hänsel, F.; Poliak, J.; Hübner, M.; Beisel, D.; Becker, U.; Schnieder, E.: Reference Platforms for the Certification of Satellite Based Localisation Systems in Transportation. Tagungsband Eurnex-Zel, Zilina (SK), 2007.

[Hänsel 2008] Hänsel, F.: Zur Formalisierung technischer Normen. Dissertation, Technische Universität Braunschweig, Institut für Verkehrssicherheit und Automatisierungstechnik, VDI-Verlag, 2008.

[Hartwig et al. 2005] Hartwig, K.; Grimm, M.; Meyer zu Hörste, M.; Lemmer, K.: Safety Relevant Positioning Application in Rail Traffic using the European Satellite System „Galileo“. Tagungsband CERGAL, Braunschweig, 2005.

[Hinzen 1993] Hinzen, A.: Der Einfluss des menschlichen Fehlers auf die Sicherheit der Eisenbahn. Dissertation, Verkehrswissenschaftliches Institut der RWTH Aachen, 1993.

[Holzmann 2004] Holzmann, G., Marks-Fährmann, U., Sudwischer, K.-H.: Grundwissen Bahn. Verlag Europa-Lehrmittel, Haan-Gruiten, 2004.

[Illgen et al. 2000] Illgen, I.; Bikker, G.; Kaiser, M.; Schnieder, E.: SATNAB a satellite-based ground experiment, Location and dynamic reference with only one satellite in guided traffic. GNSS 2000, Edinburgh, Mai 2000.

[Kiriczi 1996] Kiriczi, S.: Signaltechnisch sichere Fehlergrenzen für die Erfassung der Bewegungszustände von Bahnen. Dissertation, Institut für Regelungs- und Automatisierungstechnik, Technische Universität Braunschweig, VDI Verlag, Düsseldorf, 1996.

[Klinge 1997] Klinge, K.-A.: Konzept eines fahrzeugautarken Ortungsmoduls für den spurgebundenen Verkehr. Dissertation, Institut für Regelungs- und Automatisierungstechnik, Technische Universität Braunschweig, Shaker Verlag, 1997.

[König 2050] König, S.: König, S.: Middleware für evolutionäre Architekturen und Anwendung für ein kooperatives Produktionskonzept im Schienen-güterverkehr. Dissertation, Technische Universität Braunschweig, Institut für Verkehrssicherheit und Automatisierungstechnik, 2005.

[Kupke 2007] Kupke, T.: Funkbasierte energieautarke Kommunikation für Eisenbahngüterzüge. Dissertation, Technische Universität Braunschweig, 2007.

[Lang et al. 2002] Lang, G., Junker, K., Wurster, K., Wegel, H.: Systemverfügbarkeit und Pünktlichkeit im Bahnbetrieb. In ETR – Eisenbahntechnische Rundschau, November 2002.

[Leinhos 1996] Leinhos, D.: Analyse und Entwurf von Ortungssystemen für den Schienenverkehr mit strukturierten Methoden. Dissertation, Technische Universität Braunschweig, Institut für Regelungs- und Automatisierungs-technik, VDI Verlag GmbH, Düsseldorf, 1996.

[Lenz 1999] Lenz, W.: Reaktivierung von Schienennebenstrecken durch den Einsatz satellitengestützten Zugleitbetriebs, Diplomarbeit Universität Stuttgart, Stuttgart, 1999.

[LOCOPROL 2005] Marais, J.: Train Protection, Control and Command – LOCOPROL, Projektbericht, INRETS (F), 2005.

[Lübke 2008] Lübke, D.; Siegmann, J. (Hrsg.): Handbuch – Das System Bahn. Eurailpress-Verlag, 2008.

[Marais et al. 2003] Marais, J.; Berbineau, M.; Frimat, O.; Franckart, J.-P.: A new satellite-based fail-safe train control and command for low density railway lines, Villeneuve d'Ascq, 2003.

[May 2002] May, J.: Risikoanalyse mittels formaler Technik im Rahmen von EN 50126 aus Sichtweise eines Eisenbahnunternehmens (SBB AG) bei Einführung von ETCS. Diplomarbeit, Technische Universität Braunschweig, August 2002.

[Meyer zu Hörste 2004] Meyer zu Hörste, M.: Methodische Analyse und generische Modellierung von Eisenbahnleit- und Sicherungssystemen. Dissertation, Technische Universität Braunschweig, VDI-Verlag, 2004.

[Meyer zu Hörste 2007] Meyer zu Hörste, M.: DemoORT – Sicherheitsrelevante Ortung mit GNSS bei der Eisenbahn. Konferenzbeitrag GNSS-ZEL, Zilina (SK), 2007.

[Müller 2006] Müller, L., Schnieder E.: Prozessoptimierung als Beitrag zur Sicherheitskultur in der Eisenbahnindustrie. In ETR – Eisenbahntechnische Rundschau, Oktober 2006.

[Naumann/Pachl 2004] Naumann, P.; Pachl, J.: Leit- und Sicherungstechnik im Bahnbetrieb; Fachlexikon., 2. Auflage, Tetzlaff Verlag, Hamburg, 2004.

[Oetting 2008] Oetting, A.: FreeFloat steigert Kapazität und Pünktlichkeit. In Netznachrichten der DB Netze, Sept. 2008.

[Pachl 2004] Pachl, J.: Systemtechnik des Schienenverkehrs; Bahnbetrieb planen, steuern und sichern; Verlag B.G. Teubner, Stuttgart, Leipzig, Wiesbaden, 4. Auflage, 2004.

[Pachl 2004-1] Pachl, J.: Vorschlag für eine neue Systematik der Betriebsverfahren deutscher Eisenbahnen. In EI – Eisenbahn Ingenieur (55), Juli 2004.

[Pachl 2005] Pachl, J.: Entwicklung der Leit- und Sicherungstechnik für das System Bahn. In ETR – Eisenbahntechnische Rundschau, März 2005.

[Poliak 2009] Poliak, J.: Validierung von GNSS basierten Ortungssystemen. Dissertation, Institut für Verkehrssicherheit und Automatisierungstechnik, Technische Universität Braunschweig, 2009.

[Quante et al. 2000] Quante, F.; Leißner, F.; Ptok, B.; Seyfarth, H.-J.: Untersuchungen zur Zugvollständigkeitsüberwachung (ZVS) für Güterzüge; in ETR – Eisenbahntechnische Rundschau, Juli/August 2000.

[Reinhold 2009] Reinhold, T.: Quo vadis Deutsche Bahn? In Internationales Verkehrswesen, S. 182, Eurailpress, Mai 2009.

[Sanftleben et al. 2001] Sanftleben, D.; Sonntag, H.; Weber, K.: Verfahren „Energiesparende Fahrweise“. In ETR – Eisenbahntechnische Rundschau, Sept. 2001.

[Scheppan 2006] Scheppan, M.: Zugleitbetrieb für einfache betriebliche Verhältnisse. Verlagsgruppe Deutscher Verkehrs-Verlag, Hamburg, 2006.

[Schivelbusch 1977] Schivelbusch, W.: Geschichte der Eisenbahnreise, Zur Industrialisierung von Raum und Zeit im 19. Jahrhundert. Carl Hanser-Verlag, München, 1977.

[Schneeweiss 1999] Schneeweiss, W.: Die Fehlerbaummethode (aus dem Themenkreis. Zuverlässigkeits- und Sicherheitstechnik). LiLoLe-Verlag, Hagen, 1999.

[Schnieder 1999] Schnieder, E.: Methoden der Automatisierung. Vieweg & Sohn Verlagsgesellschaft, Braunschweig/Wiesbaden, 1999.

[Schnieder 2003] Schnieder, E.: Beschreibung der Verlässlichkeit von Verkehrssystemen im Verfügbarkeits-Sicherheits-Diagramm. In Signal und Draht, Oktober 2003.

[Schnieder 2007] Schnieder, E., Hrsg.: Verkehrsleittechnik – Automatisierung des Straßen- und Schienenverkehrs. Springer Verlag, Berlin u.a., 2007.

[Schnieder 2008] Schnieder, E., Schnieder, L.: Axiomatik der Begriffe für die Automatisierungstechnik. In: atp – Automatisierungstechnische Praxis 10 (2008).

[Schnieder 2009] Schnieder, L.; Schnieder, E.: Präzisierung des normativen Sicherheitsbegriffs durch formalisierte Begriffsbildung. In: Acatech, Hrsg.: Sicherheitsforschung – Chancen und Perspektiven, Springer-Verlag Berlin Heidelberg, 2009.

[Schnieder L 2009] Schnieder, L.: Formalisierte Terminologien technischer Systeme und ihrer Zuverlässigkeit. Dissertation, Technische Universität Braunschweig, 2010.

[Schnieder/Barbu 2009] Schnieder, E.; Barbu, G.: Potenziale satellitenbasierter Ortung für Eisenbahnen. In ETR – Eisenbahntechnische Rundschau, Januar/Februar 2009.

[Schröder 2009] Schröder, J.: Von der Menschlichen zur Technischen Zuverlässigkeit bei Betriebsverfahren für Nebenbahnen. In Tagungsband: Tagung Technische Zuverlässigkeit, Leonberg, April 2009.

[Schwanhäußer 2009] Schwanhäußer, Wulf; Wirtschaftlich und betrieblich optimale Zugzahlen auf Eisenbahnstrecken. In ETR – Eisenbahntechnische Rundschau, 2009.

[Selcat 2007] Slovak, R.: SELCAT – A new European project for level crossings. Tagungsband "6th International Exhibition & Seminars on Rail Technology", 2007.

[Six 1996] Six, J.: Abstandshaltung und Streckenleistungsfähigkeit. In Signal und Draht, April 1996.

[Slovak 2007] Slovak, R.: Methodische Modellierung und Analyse von Sicherungssystemen des Eisenbahnverkehrs. Dissertation, Institut für Verkehrssicherheit und Automatisierungstechnik, Technische Universität Braunschweig, 2007.

[Stadlmann 2008] Stadlmann, Burkhard; Moderne Zugsteuerung für den Zugleitbetrieb auf der Linzer Lokalbahn – Ein Erfahrungsbericht. Tagungsbeitrag „RegioMove 2008", Mürzzuschlag (A), 2008.

[Ständer et al. 2007] Ständer, T.; Drewes, J.; Braun, I.; Schnieder, E.: A Semi-Formal Condition-Event-Net-Based-Approach for Proving Operational Safety of Transport Systems. In: Schnieder, E.; Tarnai, G., Hrsg.: Proceedings of the 6th International Symposium FORMS/FORMAT – Formal Methods for Automation and Safety in Railway and Automotive Systems, Technische Universität Braunschweig, Januar 2007.

[Stanley/Stutzbach 2006] Stanley, P., Stutzbach, J.: Optimierung von Kosten und Sicherheit durch geeignete Nutzung der EN. In Signal und Draht, März 2006.

[Suckale 2006] Suckale, M.: Kompendium Eisenbahngesetze. Eurailpress-Verlag, 14. Auflage 2006.

[Suwe 2000] Suwe, K.-H.: Die Arbeitsweise des Eisenbahn-Bundesamtes bei der Zulassung am Beispiel von Signalanlagen; in VDI-Berichte 1546 – Sicherheit komplexer Verkehrssysteme, VDI Verlag, Düsseldorf, 2000.

[Theeg 2009] Theeg, G.; Vlasenko, S. (Hrsg.): Railway Signalling & Interlocking, International Compendium. Eurail-Press-Verlag, Hamburg, 2009.

[Thiele 2008] Thiele, L.: Untersuchung von Wirtschaftlichkeitsaspekten der Ortung im Schienenverkehr. Diplomarbeit. Institut für Verkehrssicherheit und Automatisierungstechnik, Technische Universität Braunschweig, 2008.

[Urech et al. 2002] Urech, A.; Diestro, J. P.; González, O.: GADEROS – A Galileo Demonstrator for Railway Operation System. Tagungsband DASIA, Dublin (Irland) Mai 2002.

[Verkehr 2007] Verkehr in Zahlen 2006/2007 (Taschenbuch). Hrsg.: Bundesministerium f. Verkehr, 2007.

[Wegele 2005] Wegele, S.: Echtzeitoptimierung für die Disposition im Schienenverkehr. Dissertation, Technische Universität Braunschweig, Institut für Verkehrssicherheit und Automatisierungstechnik, 2005.

[Wittenberg 2002] Wittenberg, K.-D.: Sicherheits- und Betreiberverantwortung – Teil 1. In Signal und Draht, (Dez. 2001), 2002.

[Wittenberg et al. 2004] Kommentar zum Allgemeinen Eisenbahngesetz (AEG). 1. Auflage, Eurailpress-Verlag, 2004.

[Wittenberg et al. 2006] Kommentar zur Eisenbahn-Bau- und Betriebsordnung (EBO). 5. Auflage, Eurailpress-Verlag, 2006.

[Zimmer 2002] Zimmer, C.: Konzeptioneller Neuansatz für den Betrieb von Nebenstrecken. In EI – Eisenbahningenieur, Dezember 2002.

Gesetze, Richtlinien und Verordnungen:

[AEG 2008] Allgemeines Eisenbahngesetz (AEG). Internet: http://bundesrecht.juris.de/bundesrecht/aeg_1994/gesamt.pdf; 11.12.2008.

[BGB] Bürgerliches Gesetzbuch (BGB). Internet: http://bundesrecht.juris.de/bundesrecht/bgb/gesamt.pdf; 11.12.2008.

[EBO 2008] Eisenbahn-Bau- und Betriebsordnung (EBO). Internet: www.rechtliches.de/info_EBO.html; 05.04.2008.

[TEIV 2007] Verordnung über die Interoperabilität des transeuropäischen Eisenbahnsystems (Transeuropäische-Eisenbahn-Interoperabilitätsverordnung TEIV); Internet; http://bundesrecht.juris.de/bundesrecht/teiv/gesamt.pdf; vom 05.07.2007.

[VDI/VDE 3542] VDI/VDE 3542 – Richtlinie: Sicherheitstechnische Begriffe für Automatisierungssysteme. In 4 Blättern, Beuth Verlag GmbH, 10/2000.

[VDI/VDE 3681] VDI/VDE 3681 – Richtlinie: Einordnung und Bewertung von Beschreibungsmitteln aus der Automatisierungstechnik. Beuth Verlag GmbH, 2005.

[VDI/VDE 3682] VDI/VDE 3682 – Richtlinie: Formalisierte Prozessbeschreibung. Beuth Verlag GmbH, 2005.

[91/440/EG 1991] Europäische Richtlinie 91/440/EG – Richtlinie über die Vorverlagerung des freien Marktzugangs für den internationalen Eisenbahngüterverkehr, 1991.

[2004/49/EG 2004] Europäische Richtlinie 2004/49/EG – Richtlinie über die Eisenbahnsicherheit, 2004.

[2009/352/EG 2009] Europäische Verordnung Nr. 352/2009 der Kommission vom 24. April 2009 über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken, 2009.

[Mü 8004] Technische Grundsätze für die Zulassung von Sicherungsanlagen, Eisenbahn-Bundesamt, München, Ausgabe 01.08.2003.

Normen:

[IEC 60300-3-1] Norm IEC 60300: Zuverlässigkeitsmanagement – Teil 3-1: Anwendungsleitfaden – Verfahren zur Analyse der Zuverlässigkeit – Leitfaden zur Methodik (IEC 60300-3-1:2003). Deutsche Fassung EN 60300-3-1:2004.

[IEC 61025] Norm IEC 61025: Fehlzustandsbaumanalyse; Fehlerbaumanalyse (FTA). Deutsche Fassung 2007.

[IEC 61508] Norm IEC 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbar elektronischer Systeme. Deutsche Fassung DIN EN 61508, 2001.

[IEC 62551] Norm DIN IEC 62551: Analysemethoden für Zuverlässigkeit – Petrinetz-Modellierung. Deutsche Fassung, 2008.

[EN 50121] Norm DIN EN 50121: Bahnanwendungen – Elektromagnetische Verträglichkeit – Teil 2: Störaussendungen des gesamten Bahnsystems in die Außenwelt. Deutsche Fassung EN 50121-2: 2006.

[EN 50126] Norm DIN EN 50126: Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS). CENELEC, Deutsche Fassung EN 50126: 1999.

[EN 50128] Norm DIN EN 50128: Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme. CENELEC, Deutsche Fassung EN 50128: 2001.

[EN 50129] Norm DIN EN 50129: Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik. CENELEC, Deutsche Fassung EN 50129: 2003.

[EN 50155] Norm DIN EN 50155: Bahnanwendungen – Elektronische Einrichtungen auf Bahnfahrzeugen. CENELEC, Deutsche Fassung EN 50155: 2007.

[EN 50159] Norm DIN EN 50159: Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Teil 1: Sicherheitsrelevante Kommunikation in geschlossenen Übertragungssystemen. CENELEC, Deutsche Fassung EN 50159-1: 2001.

[EN 60812] Deutsche Norm EN 60812: Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlzustandsart- und -auswirkungsanalyse (FMEA) (IEC 60812: 2006). Deutsche Fassung EN 60812: 2006.

[ISO 900x] EN ISO 9000 ff. : 2008: Qualitätsmanagement, Deutsche Fassung, 2008.

Richtlinien des Konzerns DB AG:

[RIL 408] DB Richtlinie 408 – Züge fahren und Rangieren, DB Netz AG, Stand: 30. Juni 2006.

[RIL 436] DB Richtlinie 436 – Zug- und Rangierfahrten im Zugleitbetrieb durchführen (ZLB), DB Netz AG, Stand: 30. Juni 2006.

[RIL 437] DB Richtlinie 437 – Zug- und Rangierfahrten im signalisierten Zugleitbetrieb durchführen (SZB), DB Netz AG, Stand: 30. Juni 2006.

ABKÜRZUNGSVERZEICHNIS

AEG	Allgemeines Eisenbahngesetz
ALARP	As Low As Reasonably Practicable
BGB	Bürgerliches Gesetzbuch
CENELEC	Europäisches Komitee für elektrotechnische Normung
DB AG	Deutsche Bahn AG
DemoORT	Entwicklung eines Demonstrators für Ortungsaufgaben mit Sicherheitsverantwortung im Schienengüterverkehr
DLR	Deutsches Zentrum für Luft- und Raumfahrt
EBA	Eisenbahn-Bundesamt
EBO	Eisenbahn-Bau- und Betriebsordnung
EdB	Eisenbahnen des Bundes
Ef	Eisenbahnfahrzeugführer
EIU	Eisenbahninfrastrukturunternehmen
EKA	Tagungsreihe: Entwurf komplexer Automatisierungssysteme
EMV	Elektromagnetische Verträglichkeit
EN	Europäische Norm
ERTMS	European Rail Traffic Management System
ETA	Event-Tree-Analysis (Ereignisbaumanalyse)
ETCS	European Train Control System
EVU	Eisenbahnverkehrsunternehmen
FFB	Funk-Fahr-Betrieb
FMECA	Failure-Mode- Effect-and-Criticality-Analysis
FMEA	Failure Mode and Effects Analysis
FTA	Fault-Tree-Analysis (Fehlerbaum- oder Störungsbaumanalyse)
GAMAB	Globalement Au Moin Aussi Bon
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM-R	Global System for Mobile Communications - Railway
IEC	International Electrotechnical Commission
IfRA	Institut für Regelungs- und Automatisierungstechnik (TU-Braunschweig)
INDUSI	Induktive Zugsicherung
iVA	Institut für Verkehrssicherheit und Automatisierungstechnik (TU-Braunschweig)

LZB	Linienförmige Zugbeeinflussung (Linienzugbeeinflussung)
MDT	mean down time
MEM	Minimale Endogene Mortalität
MMI	Man-Maschine-Interface (Mensch-Maschine-Schnittstelle)
MRT	Institut für Mess- und Regelungstechnik der Universität Karlsruhe
MUT	mean up time
PTB	Physikalisch Technische Bundesanstalt
Radar	Radio Detection and Ranging
RAMS	Reliability, Availability, Maintainability, Safety
RCAS	Railway Collision Avoidance System
RFID	Radio Frequency Identification
RIL	Richtlinie
RPZ	Risikoprioritätszahl
SELCAT	Safer European Level Crossing Appraisal and Technology
SIL	Safety Integrity Level
SSAS	Softwaresicherheitsanforderungsstufe
SZB	Signalisierter Zugleitbetrieb
TEIV	Verordnung über die Interoperabilität des transeuropäischen Eisenbahnsystems
THR	Tolerable Hazard Rate
UIC	Union Internationale des Chemins de Fer (Internationaler Eisenbahnverband)
USV	Unterbrechungsfreie Stromversorgung
VDE	Verband der Elektrotechnik und Elektronik
VDI	Verband Deutscher Ingenieure
XML	Extensible Markup Language
ZL	Zugleiter
ZLB	Zugleitbetrieb